System health

Published: 2020-05-19

The System Health page provides a large collection of charts that enable you to make sure that your appliance is running as expected, to troubleshoot issues, and to assess areas that are affecting performance. For example, you can monitor the number of packets processed by the ExtraHop system to ensure that packets are continuously captured.

Note: The ExtraHop Admin UI also provides status information and diagnostic tools for all ExtraHop systems.

Navigate the System Health page

Access the System Health page by clicking the System Settings icon. The System Health page automatically displays information about the ExtraHop system you are connected to. If you are viewing the System Health page from a Command appliance, you can select any connected Discover appliance from the View Appliance drop-down menu at the top of the page.

Charts on the System Health page are divided into the following sections:

Device Discovery

View the total amount of devices on your network. See which devices have been discovered and how many of those devices are currently active.

Data Feed

Assess the efficiency of the wire data collection process with charts related to throughput, packet rate, desyncs, and capture drops.

Triggers

Monitor the impact of triggers on your system. See how often triggers are running, how often they are failing, and which triggers are placing the largest load on your CPU.

Open Data Streams (ODS)

Follow the activity of open data stream (ODS) transmissions to and from your system. View the total number of remote connections, message throughput, and details related to specific remote targets.

SSL Certificates

Review the status information for all SSL certificates on your system.

Remote Packet Capture (RPCAP)

View the number of packets and frames that are sent and received by RPCAP peers.

Advanced Health Metrics

Track heap allocation related to data capture, the system datastore, triggers, and remote transmissions. Monitor write throughput, working set size, and trigger activity on the system datastore.

Device Discovery

The Device Discovery section of the System Health page provides a view of the total amount of devices on your network. See which types of devices are connected and how many of those devices are currently active.

The Device Discovery section provides the following charts:

- Active Devices
- Total Devices

Active Devices

An area chart that displays the number of L2, L3, gateway, and custom devices that have been actively communicating on the network over the selected time interval. Next to the area chart there is also a value chart that displays the number of L2, L3, gateway, and custom devices that were active over the selected time interval.

How this information can help you

Monitor this chart after making SPAN configuration changes to ensure that there were no unintended consequences that could put the ExtraHop system in a bad state. For example, accidental inclusion of a network can strain the capacity of the ExtraHop system capabilities by consuming more resources and requiring more packet handling, which results in poor performance. Check that the ExtraHop system is monitoring the expected number of active devices.

Total Devices

A line chart that displays the total number of L2, L3, gateway, and custom devices monitored by the ExtraHop system, whether active or inactive, over the selected time interval. Next to the area chart there is also a value chart that displays the total number of L2, L3, gateway, and custom devices that are currently being monitored by the ExtraHop system.

How this information can help you

Monitor this chart after making SPAN configuration changes to ensure that there were no unintended consequences that could put the ExtraHop system in a bad state. For example, accidental inclusion of a network can strain the capacity of the ExtraHop system capabilities by consuming more resources and requiring more packet handling, which results in poor performance. Check that the ExtraHop system contains the expected number of total devices.

Data Feed

The Data Feed section of the System Health page allows you to observe the efficiency of the wire data collection process with charts related to throughput, packet rate, desyncs, and capture drops.

The Data Feed section provides the following charts:

- Throughput
- Packet Rate
- Analyzed Flows
- Desyncs
- Capture Drop Rate
- Metrics Written to Disk (Log Scale)
- Metric Data Lookback Estimates

Throughput

An area chart depicting the throughput of incoming packets over the selected time interval, expressed in bytes per second. The chart displays throughput information for analyzed and filtered packets, as well as L2 and L3 duplicates.

How this information can help you

Exceeding product thresholds might result in data loss. For example, a high throughput rate might result in packets dropped at the span source or at a span aggregator. Similarly, large amount of L2 or L3 duplicates can also indicate an issue at the span source or span aggregator and might result in skewed or incorrect metrics.

The acceptable rate of bytes per second depends on your product. Refer to the Datasheets page to discover what the limits are for your ExtraHop Discover appliance and determine if the rate of bytes per second is too high.

Packet Rate

An area chart that displays the rate of incoming packets, expressed in packets per second. The chart displays packet rate information for analyzed and filtered packets, as well as L2 and L3 duplicates.

How this information can help you

Exceeding product thresholds might result in data loss. For example, a high packet rate might result in packets dropped at the span source or at a span aggregator. Similarly, large amounts of L2 or L3 duplicates can also indicate an issue at the span source or span aggregator and might result in skewed or incorrect metrics.

The acceptable rate of packet per second depends on your product. Refer to the Datasheets page to discover what the limits are for your ExtraHop Discover appliance and determine if the rate of packets per second is too high.

Analyzed Flows

A line chart that displays the number of flows that the ExtraHop system analyzed over the selected time interval. The chart also displays how many unidirectional flows occurred over the same time period. Next to the line chart there is a value chart that displays the total number of analyzed and unidirectional flows that occurred over the selected time interval. A flow is a set of packets that are part of a transaction between two endpoints over a protocol such as TCP, UDP, or ICMP.

How this information can help you

Exceeding product thresholds might result in data loss. For example, a high number of analyzed flows could result in packets dropped at the span source or at a span aggregator.

Desyncs

A line chart that displays occurrences of system-wide desyncs on the ExtraHop Discover appliance over the selected time interval. Next to the line chart there is also a value chart that displays the total number of desyncs that occurred over the selected time interval. A desync is when the ExtraHop data feed drops a TCP packet and, as a result, is no longer synchronized with a TCP connection.

How this information can help you

Large numbers of desyncs might indicate dropped packets on the monitoring interface, SPAN, or network tap.

If adjustments to your SPAN do not reduce a large number of desyncs, contact ExtraHop Support.

Capture Drop Rate

A line chart that displays the percentage of packets dropped at the network card interface on an ExtraHop Discover appliance over the selected time interval.

How this information can help you

Packet drops often result when appliance thresholds are exceeded. Refer to the Datasheets page to discover what the limits are for your ExtraHop Discover appliance.

Metrics Written to Disk (Log Scale)

A line chart that displays the amount of space consumed by metrics that were written to disk over the selected time interval, expressed in bytes per second. Because there is a large range between data points, the disk usage is displayed in logarithmic scale.

How this information can help you
It is important to stay aware of the amount of space that metrics are consuming on your datastore. The amount of space in your datastore will affect the amount of available lookback. If some metrics are consuming too much space, you can investigate associated triggers to see if you can modify the trigger to make it more efficient.

Metric Data Lookback Estimates

Displays the estimated datastore lookback metrics on the ExtraHop Discover appliance. Lookback metrics are available in 24 hour, 1 hour, 5 minute, and 30 second time intervals based on the write throughput rate, which is expressed in bytes per second.

How this information can help you

Refer to this chart to determine how far back you are able to look up historical data for given time intervals. For example, you might be able to look up 1 hour intervals of data as far back as 9 days.

Triggers

The Triggers section of the System Health page allows you to monitor the impact of triggers on your system. See how often triggers are running, how often they are failing, and which triggers are placing the largest load on your CPU.

The Triggers section provides the following charts:

- Trigger Load
- Trigger Executes and Drops
- Trigger Details
- Trigger Load by Trigger
- Trigger Executes by Trigger
- Trigger Exceptions by Trigger
- Trigger Cycles by Thread

Trigger Load

A line chart that displays the percentage of cycles on the ExtraHop Discover appliance that are consumed by triggers over the selected time interval, based on the total capture thread time.

How this information can help you
Look for spikes or upward growth of the trigger load, especially after creating a new trigger or modifying an existing trigger. If you notice either condition, view the Trigger Load by Trigger chart to see which triggers are consuming the most resources.

Trigger Executes and Drops

A line and column chart where the line chart displays the number of times triggers were run, and the accompanying column chart displays the number of times triggers were dropped, over the selected time interval. Next to the line and column chart there is also a value chart that displays the total number of trigger executes and drops that occurred over the selected time interval. These charts provide an overall snapshot of all triggers currently running on the ExtraHop Discover appliance.

How this information can help you
Look for spikes in the line and column chart and investigate any triggers that have resulted in the surge. For example, you might notice increased activity if a trigger has been modified or a new trigger has been enabled. View the Trigger Executes by Trigger chart to see which triggers are running most frequently.

Trigger Details

A list chart that displays individual triggers and the number of cycles, executes, and exceptions attributed to each over the selected time interval. By default, the list of triggers is sorted in descending order by trigger cycles.

How this information can help you

Identify which triggers are consuming the most cycles. Triggers that execute too frequently or otherwise consume more cycles than they should might be assigned to more sources than necessary. Make sure that any overactive trigger is only assigned to the specific source that you need to collect data from.

Trigger Load by Trigger

A line chart that displays the percentage of cycles on the ExtraHop Discover appliance that are consumed by triggers over the selected time interval, based on the total capture thread time.

How this information can help you

Identify which triggers are consuming the most cycles. Triggers that consume more cycles than they should might be assigned to more sources than necessary. Make sure that any overactive trigger is only assigned to the specific source that you need to collect data from.

Trigger Executes by Trigger

A line chart that displays the number of times each active trigger ran over the selected time interval.

How this information can help you

Look for triggers that are running more frequently than you would expect, which might indicate that the trigger is assigned too broadly. A trigger assigned to all applications or all devices might have a heavy performance cost. A trigger assigned to a device group that has been expanded might collect metrics you do not want. To minimize performance impact, a trigger should be assigned only to the specific sources that you need to collect data from.

High activity might also indicate that a trigger is working harder than it needs to. For example, a trigger might run on multiple events where it would be more efficient to create separate triggers, or a trigger script might not adhere to recommended scripting guidelines as described in the Triggers Best Practices Guide.

Trigger Exceptions by Trigger

A line chart that displays the number of unhandled exceptions, sorted by trigger, that occurred on the ExtraHop Discover appliance over the selected time interval.

How this information can help you

Trigger exceptions are the primary cause of trigger performance issues. If this graph indicates a trigger exception has occurred, you should investigate the trigger immediately.

Trigger Cycles by Thread

A line chart that displays the number of trigger cycles consumed by triggers for a thread.

How this information can help you

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. Look for an even amount of cycle consumption among threads.

Open Data Streams (ODS)

The Open Data Streams (ODS) section of the System Health page enables you to follow the activity of ODS transmissions to and from your system. You can also view the total number of remote connections, message throughput, and details related to specific remote targets.

The Open Data Streams (ODS) section provides the following charts:

- Message Throughput
- Messages Sent
- ODS Target Details
- ODS Connections
- Messages Dropped
- Message Queue Length

Message Throughput

A line chart that displays the throughput of remote message data, expressed in bytes. Next to the line chart there is also a value chart that displays the average throughput rate of remote message data over the selected time interval. Remote messages are transmissions sent to third-party systems from the ExtraHop Discover appliance through an open data stream (ODS).

How this information can help you

Monitor this chart to make sure that bytes are being transferred as expected. If you are seeing low throughput numbers, there might be an issue with the configuration of an ODS or an ODS trigger. Significant dips in throughput might indicate problems with your data streams.

Messages Sent

A line and column chart where the line chart displays the number of messages that were sent out to remote, third-party systems from the ExtraHop Discover appliance through an open data stream (ODS) and the accompanying column chart displays the number of errors that occurred during the transmission of data to the remote system. Next to the line and column chart there is also a value chart that displays the total number of messages sent out and the total number of send errors that occurred over the selected time interval.

How this information can help you

Monitor this chart to make sure that packets are sent as expected. If no packets are sent, there might be an issue with the configuration of an open data stream or an open data stream trigger. Transmission errors might involve the following:

Parse errors

Messages that are not sent due to encoding issues in the trigger script. Make sure that your ODS triggers are configured correctly.

Mismatched targets

Messages that are not sent because the name of the remote system specified in the trigger script does not match the name configured in the Admin UI. Make sure that the names of remote systems are consistent in trigger scripts and the Admin UI.

Queue full

Messages that are not sent because the message queue is full. A full queue occurs when the remote system cannot handle the current message rate. Look at the Message Queue Length and the ODS Target Details charts to see if your transmission errors might be related to a long message queue length.

ODS Target Details

A list chart that displays the following metrics for related to remote targets of an open data stream (ODS) over the selected time interval: target message send errors, off box connection errors, number of messages dropped because queue full, and IPC message decoding errors.

How this information can help you

If you are seeing message errors reported in the Messages Sent chart, the details in this chart can help you determine the root cause of ODS message errors.

ODS Connections

A line and column chart where the line chart displays the number of attempts the system made to connect to a remote system and the accompanying column chart displays the number of errors that occurred as a result of those attempts. Next to the line and column chart there is also a value chart that displays the total number of connection attempts and connection errors that occurred over the selected time interval.

How this information can help you
Identify remote targets that are requiring an unusual amount of connection attempts or generating a disproportionate amount of connection errors.

Messages Dropped

A line chart that breaks down the number of remote messages dropped into two key root causes: because the ExtraHop system internal message queue was full, and because the name of the remote system specified in the trigger script does not match the name configured in the Admin UI. Next to the line chart there is also a value chart that displays the total number of messages dropped due to a full message queue and the total number of messages dropped due to a mismatched target name over the selected time interval.

How this information can help you
If messages are being dropped due to mismatched target names, make sure that the names of remote systems are consistent in trigger scripts and the Admin UI.

Dropped messages might also indicate that the ExtraHop Discover appliance is sending data faster than the remote system can process. A long queue can cause messages to drop. Look at the Message Queue Length and the ODS Target Details charts to see if your dropped messages might be related to a long message queue length.

Message Queue Length

A line chart that displays the number of messages in a remote target's interprocess communication (IPC) queue. Messages in the queue arrived through an open data stream(ODS) from the ExtraHop Discover appliance and are waiting to be processed by the remote target.

How this information can help you
A long message queue might indicate that the Discover appliance is sending data faster than the remote system can process and could result in dropped messages. Refer to the Messages Dropped chart to determine if message drops have occurred.

SSL Certificates

The SSL Certificates section of the System Health page allows you to review the status information for all SSL certificates on your system.

The SSL Certificates section provides the following chart:

- Certificate Details

Certificate Details

A list chart that displays the following information for each certificate:

Decrypted Sessions
The number of sessions that were successfully decrypted.

Unsupported Sessions
The number of sessions that could not be decrypted with passive analysis, such as DHE key exchange.

Detached Sessions
The number of sessions that were not decrypted or only partially decrypted due to desyncs.

Passthrough Sessions

The number of sessions that were not decrypted due to hardware errors, such as those caused by exceeding the specifications of SSL acceleration hardware.

Sessions Decrypted with Shared Secret

The number of sessions that were decrypted through a shared secret key.

How this information can help you

Monitor this page to make sure that the correct SSL certificates are installed on the ExtraHop Discover appliance and are performing decryption as expected.

Remote Packet Capture (RPCAP)

The Remote Packet Capture (RPCAP) section of the System Health page enables you to view the number of packets and frames that were sent from RPCAP peers and received by an ExtraHop appliance.

The Remote Packet Capture (RPCAP) section provides the following charts:

- Forwarded by Peer
- Received by Appliance

Forwarded by Peer

A list chart that displays the following information regarding packets and frames that are forwarded by an RPCAP peer:

Forwarded Packets

The number of packets that an RPCAP peer attempted to forward to an ExtraHop appliance.

Forwarder Interface Frames

The total number of packets that were viewed by the forwarder. Forwarders on RPCAP devices will coordinate with each other to keep multiple devices from sending the same packet. This is the number of packets that were viewed before any frames were removed to reduce forwarded traffic, and before frames were removed by user-defined filters.

Forwarder Kernel Frame Drops

The number of frames that were dropped because the kernel of the RPCAP peer was overloaded with the stream of unfiltered frames. Unfiltered frames have not been filtered by the kernel to remove duplicate packets or packets that should not be forwarded because of user-defined rules.

Forwarder Interface Drops

The number of packets that were dropped because the RPCAP forwarder was overloaded with the stream of unfiltered frames. Unfiltered frames have not been filtered to remove duplicate packets or packets that should not be forwarded because of user-defined rules.

How this information can help you

Any time you see packets dropped by the RPCAP peer, it indicates that there is an issue with the RPCAP software.

Received by Appliance

A list chart that displays the following information regarding packets and frames that are received by an ExtraHop system from a Remote Packet Capture (RPCAP) peer:

Encapsulated Bytes

The total size of all packets related to the UDP flow from the RPCAP device to the ExtraHop system, in bytes. This information shows you how much traffic the RPCAP forwarder is adding to your network.

Encapsulated Packets

The number of packets related to the UDP flow from the RPCAP device to the ExtraHop appliance.

Tunnel Bytes

The total size of packets, not including encapsulation headers, that the ExtraHop appliance received from an RPCAP device, in bytes.

Tunnel Packets

The number of packets that the ExtraHop system received from an RPCAP peer. This number should be very close to the Forwarded Packets number in the Sent by Remote Device chart. If there is a big gap between these two numbers, then packets are dropping between the RPCAP device and the ExtraHop system.

How this information can help you

Tracking the encapsulated packets and bytes is a good way to make sure that RPCAP forwarders are not placing an unnecessary load on your network. You can monitor tunnel packets and bytes to make sure that the ExtraHop system is receiving everything that the RPCAP device is sending.

Advanced Health Metrics

The Advanced Health Metrics section of the System Health page allows you to track heap allocation related to data capture, the system datastore, triggers, and remote transmissions. Monitor write throughput, working set size, and trigger activity on the system datastore.

The Advanced Health Metrics section provides the following charts:

- Capture and Datastore Heap Allocation
- Trigger and Remote Heap Allocation
- Store Write Throughput
- Working Set Size
- Datastore Trigger Load
- Datastore Trigger Executes and Drops
- Datastore Trigger Exceptions by Trigger

Capture and Datastore Heap Allocation

A line chart that displays the amount of memory that the ExtraHop Discover appliance dedicates to network packet capture and to the datastore.

How this information can help you

The data in this chart is for internal purposes and might be requested by ExtraHop Support to help you diagnose an issue.

Trigger and Remote Heap Allocation

A line chart that displays the amount of memory, expressed in bytes, that the ExtraHop Discover appliance dedicates to processing capture triggers and to open data streams (ODS).

How this information can help you

The data in this chart is for internal purposes and might be requested by ExtraHop Support to help you diagnose an issue.

Store Write Throughput

An area chart that displays the datastore write throughput, expressed in bytes, on the ExtraHop Discover appliance. The chart displays data for the selected time interval and for 24 hour, 1 hour, 5 minute, and 30 second intervals.

How this information can help you
The data in this chart is for internal purposes and might be requested by ExtraHop Support to help you diagnose an issue.

Working Set Size

An area chart that displays the write cache working set size for metrics on the ExtraHop Discover appliance. The working set size indicates how many metrics can be written to the cache for the selected time interval and for 24 hour, 1 hour, 5 minute, and 30 second intervals.

How this information can help you
The data on this chart might spike after trigger creation or trigger modification if the trigger script is not collecting metrics efficiently.

Datastore Trigger Load

A line chart that displays the percentage of cycles consumed by datastore-specific triggers on the ExtraHop Discover appliance, based on the total capture thread time.

How this information can help you
Look for spikes or upward growth of the datastore trigger load, especially after creating a new datastore trigger or modifying an existing datastore trigger. If you notice either, click on the **Trigger Load** metric label to drill down and see which datastore triggers are consuming the most resources.

Datastore Trigger Executes and Drops

A line and column chart where the line chart displays the number of times datastore-specific triggers on the ExtraHop Discover appliance were run during the selected time interval, and the accompanying column chart displays the number of datastore-specific triggers dropped from the queue of triggers waiting to run on the ExtraHop Discover appliance during the selected time interval.

How this information can help you
A single datastore trigger that runs often might indicate that the trigger has been assigned to all sources, such applications or devices. To minimize performance impact, a trigger should be assigned only to the specific sources that you need to collect data from.

From the Datastore Trigger Load chart, click on the **Trigger Load** metric label to drill down and see which datastore triggers are running most frequently.

Any drop data displayed on the column chart indicates that datastore trigger drops are occurring and that trigger queues are backed up.

The system queues trigger operations if a trigger thread is overloaded. If the datastore trigger queue grows too long, the system stops adding trigger operations to the queue and drops the triggers. Currently running triggers are unaffected.

The primary cause of long queues, and subsequent trigger drops, is a datastore long-running trigger.

Datastore Trigger Exceptions by Trigger

A list chart that displays the number of unhandled exceptions caused by datastore-specific triggers on the ExtraHop Discover appliance.

How this information can help you
Datastore trigger exceptions are the primary cause of trigger performance issues. If this graph indicates a trigger exception has occurred, the datastore trigger should be corrected immediately.

Status and diagnostics tools in the Admin UI

The Admin UI is another source for system information and diagnostics.

For more metrics about the overall health of the ExtraHop Discover appliance, and for diagnostic tools that enable ExtraHop Support to troubleshoot system errors, look at the Status and Diagnostics section of the Admin UI.