Metrics concepts

Published: 2018-04-20

Metrics are measurements of network behavior. Metrics help you to gain visibility into what is happening in your network in real-time. In the ExtraHop system, metrics are calculated from wire data, and then associated with devices and protocols. The ExtraHop system provides a large number of metrics, which you can explore from protocol pages in the Metrics section of the ExtraHop Web UI. You can also search for metrics in the Metric Catalog, in the Metric Explorer, and by searching for metrics by source and then protocol.

Types of metrics

Each metric in the ExtraHop system is classified into a metric type. Understanding the distinctions between metric types can help you configure charts or write triggers to capture custom metrics. For example, a heatmap chart can only display dataset metrics.

Count

The number of events that occurred over a specific time period. You can view count metrics as a rate or a total count. For example, a byte is recorded as a count, and can either represent a throughput rate (as seen in a time series chart) or total traffic volume (as seen in a table). Rates are helpful for comparing counts over different time periods. A count metric can be calculated as a per-second average over time. When viewing high-precision, or 1-second, bytes and packet metrics, you can also view a maximum rate and minimum rate. Count metrics include errors, packets, and responses.

Distinct count

The number of unique events that occurred during a selected time interval. The distinct count metric provides an estimate of the number of unique items placed into a HyperLogLog set during the selected time interval.

Dataset

A distribution of data that can be calculated into percentiles values. Dataset metrics include processing time and round trip time.

Maximum

A single data point that represents the maximum value from a specified time period.

Sampleset

A summary of data about a detail metric. Selecting a sampleset metric in a chart enables you to display a mean (average) and standard deviation over a specified time period.

Snapshot

A data point that represents a single point in time.

Tip: Visit the Tip of the Week: Metric Types post on the ExtraHop community forum.

Metric sources

In the ExtraHop system, a metric is a measurement of observed network behavior. Metrics are generated from network traffic, and then each metric is associated with a source, such as an application, device, or network. When you select a source from the Metrics section of the Web UI, or in the Metric Explorer when building a chart, you can view metrics associated with that source. Each source provides access to a different collection of metrics.

Select from the following sources and groups as you configure dashboard widgets or navigate across protocol pages.

Applications

An application is a user-defined container that you can associate with multiple devices and protocols for a unified view of built-in metrics.

These containers can represent distributed applications on your network environment. For example, if you want a unified view of all the network traffic associated with a website—from web transactions to DNS requests and responses to database transactions—you can create a custom application that contains all of these related metrics.

The ExtraHop Web UI enables you to create basic applications that filter metrics by protocol. For advanced applications, you must write a trigger, which requires JavaScript code. For example, you must write a trigger to apply advanced filters for collecting metrics, to create custom application metrics, or to collect metrics from non-L7 traffic.

For more information about creating applications, see Create an application through the Web UI and Create an application through the Trigger API.

Networks

A network capture is the entry point into network devices and virtual LANs (VLANs) that are detected from wire data by the ExtraHop system. A flow network is a network device, such as a router or switch, that sends information about flows seen across the device. A flow network can have multiple interfaces.

Devices

Devices are objects on your network with a MAC address and IP address that have been automatically discovered and classified by the ExtraHop system. Metrics are available for every discovered device on your network. An L2 device has a MAC address only; an L3 device has an IP address and MAC address.

For more information about how devices are automatically discovered and classified by the ExtraHop system, see Device discovery.

Device groups

A device group is a user-defined collection of devices that can help you track metrics across multiple devices. You can create a dynamic device group by automatically adding all devices that meet matching criteria, or you can create a static device group by manually selecting individual devices.

Matching criteria for dynamic device groups can be a hostname, IP address, MAC address, or any of the filter criteria listed for the device on the Devices page. For example, you can create a dynamic group and then configure a rule to add all devices within a certain IP address range to that group automatically.

Activity groups

An activity group is a collection of devices automatically grouped together by the ExtraHop system based on network traffic. A device with multiple types of traffic might appear in more than one activity group; for example, if a CIFS client is authenticating through LDAP, the device will appear in both the CIFS Clients and the LDAP Clients activity groups. Activity groups make it easy to identify all the devices associated with a protocol, or determine which devices were associated with protocol activity during a specific time interval.

Related topics

- View the metrics available on built-in protocol pages
- Create a custom dashboard to view metrics
- Create custom metrics
- Set up a threshold alert to monitor metric activity