Metrics

Published: 2019-02-18

Metrics are real-time measurements of your network behavior that the ExtraHop system calculates from wire data. You can track network activity with dashboards and detail pages of over 4,500 metrics related to specific protocols, networks, devices, or applications.

Tip: If you have a connected Explore appliance, learn how to view transaction-level information associated with a metric. If you have a connected Trace appliance, learn how to configure the global packet capture feature to start collecting packets.

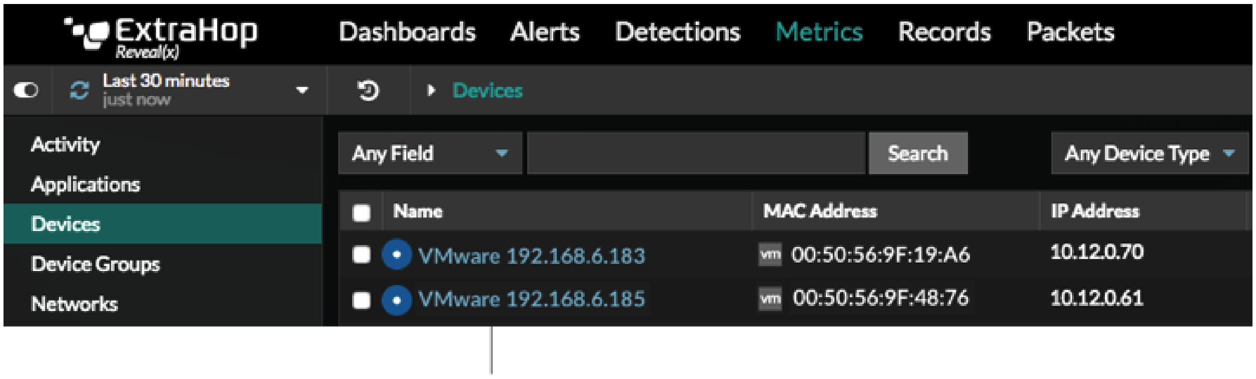
Navigate metrics

Metric pages show you your network activity through protocol pages, dashboards, and detail pages.

Protocol pages

Visit a protocol page to find specific metrics for a device, a group of devices, an application, or a network. Protocol pages include built-in charts with top-level metrics that are relevant to the protocol and source you are viewing. As you find metrics that are critical to your network success, you can copy them to create curated dashboards.

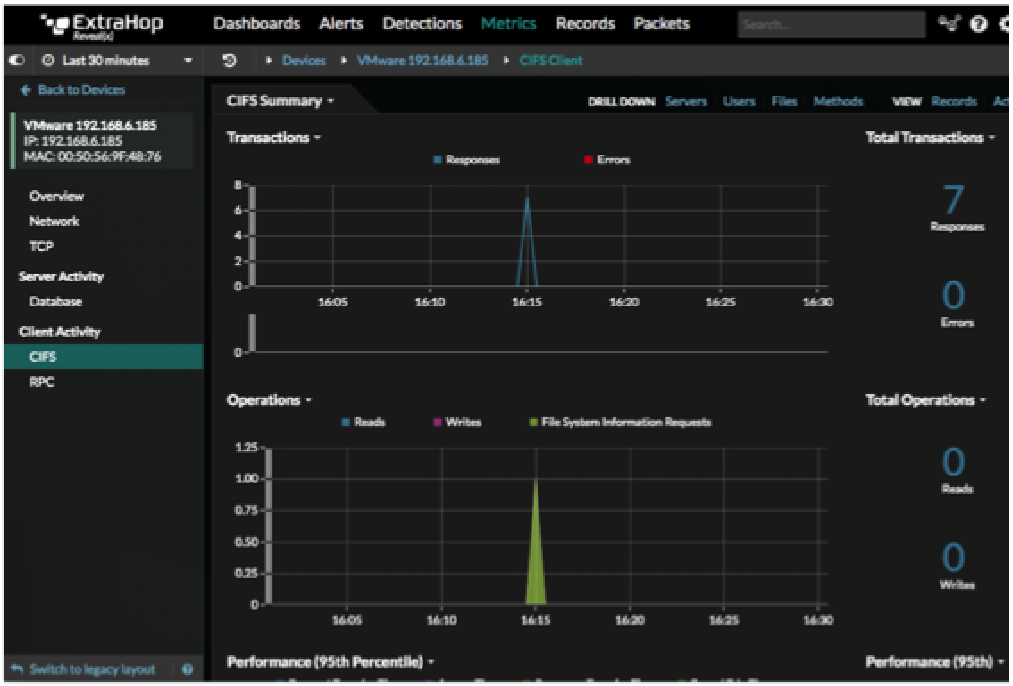
While there are many ways to access protocol pages, we recommend that you first locate a source, such as a device that you want to investigate. Then, click the source name, which is linked to a protocol page. For example, click **Metrics** at the top of the page, select a source in the left pane, and then click a source name to visit its protocol page, as shown in the following figure.



□	Name	MAC Address	IP Address
□	VMware 192.168.6.183	00:50:56:9F:19:A6	10.12.0.70
□	VMware 192.168.6.185	00:50:56:9F:48:76	10.12.0.61

Click a source name to view the protocol page

The protocol page then gives you access to all of the metrics associated with that device, as shown in the following figure.



Click a link in the side-pane to view metrics by protocol or device role

Note: You cannot change the layout of metric charts in a protocol page, but you can create a dashboard and customize the chart layout.

Dashboards

Visit a system dashboard when you want to see metrics about the general activity and health of your entire network. Or, create a dashboard with multiple chart types and unique combinations of metrics and sources.

Click **Dashboards** at the top of the page to access your custom dashboards or system dashboards. All ExtraHop users have access to the following built-in system dashboards:

- Activity dashboard
- Network dashboard
- Security dashboard - Reveal(x) only

Detail page

You can drill down on top-level metrics from protocol pages or dashboards to view detail metrics. A detail metrics page provides a list of metric values for a specific key (such as a client or server IP address). Investigate detail metrics to learn how a specific device, method, or resource is affecting the network.

Metric Catalog

All built-in and custom metrics are listed in the Metric Catalog. Click the System Settings icon ⚙ and then click **Metric Catalog**. If you need to collect custom metrics, you can write a trigger and add metadata about the custom metric to the Metric Catalog to display information in any chart where that metric is added.

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 from the Metric Explorer, 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.

Devices

Devices, also known as assets and endpoints, are objects on your network with a MAC address or IP address that have been automatically discovered and classified by the ExtraHop system. An L2 device has a MAC address only. An L3 device has an IP address and MAC address. Metrics are available for devices in Advanced Analysis and Standard Analysis.

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

Device groups

A device group is a user-defined collection that can help you track metrics and specify analysis priorities for multiple devices. You can create a static device group or dynamic device group. Dynamic device groups include criteria that determines which devices are automatically included in the group. Static device groups include devices that are manually added or removed from the group.

You can also select the following built-in system device groups as the source for charts, alerts, or triggers:

New Devices (Last 24 Hours)

This device group includes assets and endpoints that were first seen by the ExtraHop system over the last 24 hours until now. The ExtraHop system automatically discovers devices that are actively communicating on your network, which means that the device sent and received data from other devices on your network. For more information, see Device Discovery FAQ.

New Device (Last 7 Days)

This device group includes assets and endpoints that were first seen by the ExtraHop system over the last 7 days until now. The ExtraHop system discovers devices that are actively communicating on your network, which means that the device sent and received data from other devices on your network. For more information, see Device Discovery FAQ.

Vulnerability Scanners

This device group includes devices that are designated or acting as vulnerability scanners. For example, a device that sends an HTTP request associated with known scanner activity is automatically added to this device group. Any device that you manually assign the Vulnerability Scanner role to will also be automatically added to this group.

Note: If a device that typically acts like a gateway or load balancer sends an HTTP request associated with scanner activity, that device is still classified as a gateway or load balancer device.

VMware

This device group includes assets and endpoints that were automatically associated with the VMware vendor role.

Domain Controllers

This device group includes devices that are designated or acting as domain controllers. The ExtraHop system considers a device a domain controller if it has processed all of the following types of activity in the last 30 minutes:

- Kerberos server
- CIFS server
- MSRPC server

Any device that you manually assign the Domain Controller role to is also automatically added to this group.

Mobile Devices

This device group includes devices that are designated or acting as mobile devices. The ExtraHop system considers a device a mobile device if it has iOS or Android software installed. Any device that you manually assign the Mobile Device role to is also automatically added to this group.

Web Proxy Servers

This device group includes devices that are designated or acting as web proxy servers. The ExtraHop system considers a device a web proxy server if it has processed an HTTP/1.x request between a device and another server in the last 30 minutes. Any device that you manually assign the Web Proxy role to is also automatically added to this group.

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.

Activity groups

An activity group is a collection of devices that are automatically grouped by protocol traffic. A device with multiple types of traffic might be included in more than one activity group. For example, if a CIFS client is authenticating through LDAP, the device is included in both the CIFS Clients and the LDAP Clients activity groups.

Activity groups make it easy to identify and work with devices that are associated with a protocol. For example, you can complete the following tasks:

- Add an activity group, such as HTTP Servers, to a chart to monitor metrics for all of your web servers.
- Create a basic activity map from an activity group.
- Prioritize an activity group for Advanced Analysis or Standard Analysis.

Appliances

ExtraHop appliances provide a large collection of metrics that enable you to monitor and assess the system health of the appliance and to collect troubleshooting data requested by ExtraHop Support.

You can select a connected ExtraHop appliance as a metric source from the Metric Explorer and build charts to monitor data such as packet throughput, heap allocation, and dropped packets on that appliance. In addition, you can add multiple appliances to a single dashboard chart to collectively monitor health metrics for your entire ExtraHop system.

You can view all appliance health metrics from the System Health page, which you can access from the System Settings ⚙ menu. For more information,about system health charts, see System health.

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.

Count rate

The number of events that occurred over a specific time period. Count rate metrics and count metrics are calculated the same way. However, count rate metrics capture additional details that enable you to view the maximum and minimum rate for an interval. Count rate metrics include bytes and packets.

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.

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
- Metrics FAQ