ExtraHop Glossary

Published: 2016-06-10

AAA

AAA (Authentication, Authorization, and Accounting) is a framework that contains protocols that control user access and resource tracking.

Activity group

Activity groups contain devices that are automatically grouped together based on their network traffic. A device with multiple types of traffic might appear in more than one activity group.

Alert

An alert is a condition that establishes baseline values for specified metrics. If those values are exceeded, the system logs the event and sends notifications through configured channels (such as email or SNMP). The Discover appliance includes built-in alerts and you can also create custom alerts.

AMF

AMF (Action Message Format) is a format for encoding data transported between Adobe Flash clients and servers.

Application

In the ExtraHop system, applications are user-defined containers for metrics that are associated with multiple devices and protocols. These containers can represent distributed applications on your network environment. In the ExtraHop system, applications are created through the Trigger API. A default application that is available to all ExtraHop users is the All Activity application.

Application Performance Monitoring

Application performance monitoring (APM) tools enable development and application teams to observe the performance of applications. Data is collected through software agents that run on application servers, databases, and other application components. The agents can be configured to gather host-based ingress and egress transaction data, code-level stack trace inputs, and resource usage metrics such as CPU, memory, and disk.

Visit the ExtraHop website: How to compare APM tools.

Area chart

This ExtraHop chart type displays metric values as a line that connects data points over time, with the area between the line and axis filled in with color.

Bar chart

This ExtraHop chart type displays the total value of metric data as horizontal bars.

Bundle

Bundles are JSON-formatted documents that contain information about selected system configuration, such as triggers, dashboards, applications, or alerts. You can create a bundle and then transfer those configurations to another ExtraHop appliance, or save the bundle as a backup of your customizations. Bundles can also be downloaded from the ExtraHop website: ExtraHop Solution Bundles.

Candlestick chart

This ExtraHop chart type displays data calculations for a distribution of metric values over time. A line at each time interval displays three or five data points. If the line has five data points, it contains a body, middle tick mark, an upper shadow line, and a lower shadow line. If the line has three data points, it contains a middle tick mark.

CIFS

CIFS (Common Internet File System), also known as SMB (Server Message Block), is an application-level protocol that provides client access to files on a network attached storage (NAS) repository, typically in a Windows environment.

Client

A client is an application or system that accesses a service made available by a server.

Column chart

This ExtraHop chart type displays metric values as vertical bars over a specified time period.

Command appliance

The ExtraHop Command appliance (ECA) provides centralized management and reporting across multiple ExtraHop Discover appliances that can be distributed across datacenters, branch offices, and the public cloud.

Count metric type

In the ExtraHop system, this top-level metric type represents the number of events that occurred over a specific time period. You can view count metrics as a rate or a total count.

Dashboard

Dashboards are built-in or customized views of your ExtraHop metrics. Dashboards display both real-time and historic data.

Database

A relational DB (database) stores, retrieves, and manages structured information through Structured Query Language (SQL).

Dataset metric type

In the ExtraHop system, this top-level metric type represents a distribution of data that can be calculated into percentiles values.

Detail metric

Detail metrics provide you with a value for a specific key, such as a client IP address, server IP address, URI, hostname, referrer, certificate, or method. When you drill down from a top-level metric in the ExtraHop system to a detail metric, you can gain insight into how a specific device, method, or resource is affecting the network.

Device

Devices are objects on your network that have been automatically discovered and classified by the ExtraHop system. Metrics are available for every discovered device on your network.

Device discovery

Device discovery is the process by which ExtraHop builds and maintains a list of active devices associated with monitored network traffic. When the ExtraHop system detects a MAC address on the network, a L2 device entry is created in the ExtraHop system and associated with that address. When the ExtraHop system detects an ARP (Address Response Protocol) response, an L3 device entry is created in the ExtraHop system and associated with the MAC address and IP address. Based on the type of traffic, the ExtraHop system also classifies the device type and assigns a name to the device. For example, an L2 device can be a gateway device or router. L3 devices can be clients, servers, or databases. You can also create a custom device in the ExtraHop system to monitor traffic for a specific IP address.

Device group

Device groups, also known as custom groups, can be either static or dynamic. You must manually identify and assign individual devices to a static group. Alternatively, you can configure rules to automatically assign devices to a dynamic group.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol for dynamically distributing network configuration parameters.

DICOM

DICOM (Digital Imaging and Communications in Medicine) is a standard for storing biomedical images and transmitting those images over a network.

Discover appliance

The ExtraHop Discover appliance (EDA) provides the ability to analyze and visualize all of your network, application, client, infrastructure, and business data. The EDA passively collects a copy of unstructured wire data—all of the transactions on your network—and transforms this data into structured wire data.

DNS

DNS (Domain Name System) is the naming system for network hosts and resources that are connected to the Internet. DNS servers map IP addresses to hostnames.

ERSPAN

Encapsulated Remote SPAN (ERSPAN) enables you to send source traffic on one switch to a destination on another switch, while traversing a Layer 3 boundary.

Explore appliance

The ExtraHop Explore appliance (EXA) integrates with the ExtraHop Discover appliance to store transaction and flow records sent from the EDA. You can view, save, and search the structured flow and transaction information about events on your network with a simple, unified UI, with no modifications to your existing applications or infrastructure.

FIX

FIX (Financial Information eXchange) is a protocol that provides information about the real-time exchange of financial transactions.

FTP

FTP (File Transfer Protocol) is a standard network protocol for transferring files between a client and a server.

Heatmap chart

This ExtraHop chart type displays a distribution of metric data over time, where color represents a concentration of data.

Histogram chart

This ExtraHop chart type displays a distribution of metric data as vertical bars, or bins.

HL7

HL7 (Health Level-7) is a standard for exchanging electronic health information between software applications.

HTTP

HTTP (Hypertext Transfer Protocol) is an application-level protocol that retrieves web pages.

IBM MQ

IBM MQ (WebSphere MQ) is a message-queuing protocol for IBM enterprise and message middleware products.

ICA

ICA (Independent Computing Architecture) is a Citrix system protocol that transmits data between clients and servers.

iSCSI

iSCSI (Internet Small Computer Systems Interface) is an TCP-level protocol that allows SCSI commands to be sent over a local-area network (LAN) or wide-area network (WAN).

L2

The data link layer in the OSI model. In the ExtraHop system, L2 metrics provide information about the connection between two devices.

L3

The network layer in the OSI model. In the ExtraHop system, L3 metrics provide IP address information for nodes that communicate over the monitored network.

L4 (TCP)

The transport layer in the OSI model. In the ExtraHop system, L4 TCP (Transmission Control Protocol) metrics provide information about the reliable transfer of packets between a source and destination.

L7

The application layer in the OSI model. In the ExtraHop system, L7 metrics provide information about interactivity with software applications.

LDAP

LDAP (Lightweight Directory Access Protocol) is a vendor-neutral protocol that maintains and provides easy access to a distributed directory.

Read the ExtraHop blog post: What Is LDAP, and Who Needs It Anyway?

Line chart

This ExtraHop chart type displays metric values as a line, which connects a series of data points over time.

Line & column chart

This ExtraHop chart type displays metric values as a line, which connects a series of data points over time, with the option to display another metric as a column chart underneath.

List chart

This ExtraHop chart displays metric values in a list across multiple columns with optional sparklines.

Maximum metric type

In the ExtraHop system, this top-level metric type is a single data point that represents the maximum value from a specified time period.

Memcache

Memcache is a protocol that provides access to high-performance, distributed memory object caching systems over a TCP connection.

Metric

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. The ExtraHop system provides builtin, or default, metrics based on observed network traffic from wire data. You can also create custom metrics in the ExtraHop system by writing a trigger to collect metrics based on a specific event.

Metric Catalog

The Metric Catalog is a tool for viewing information about built-in and custom metrics in the ExtraHop system. You also can delete and edit custom metrics through the Metric Catalog.

Metric Explorer

The Metric Explorer is a tool for configuring dashboard charts. In the Metric Explorer, you can add multiple sources and metrics to a chart and immediately preview how metric data will appear.

MongoDB

MongoDB is an open-source document database that provides performance, availability, and scalability.

NAS

NAS (Network Attached Storage) is file-level storage repository. Clients access the repository through CIFS (Common Internet File System) or NFS (Network File System) protocols.

Network

In the ExtraHop system, a network is the entry point into the network capture, and metrics are collected for network capture attributes, network alerts, and network traffic details. These metrics provide a summary of all network activity retrieved in the capture.

NFS

NFS (Network File System) is a distributed file system protocol that provides client access to files on a network attached storage (NAS) repository, typically in a UNIX environment.

Node

In the context of a Command or Explore cluster, a node is a single physical or virtual ExtraHop Discover appliance that is a member of the cluster.

PCAP

PCAP (packet capture) consists of an application programming interface (API) for capturing network traffic and storing it to a database.

PCoIP

PCoIP (PC-over-IP) is protocol that transfers compressed and encrypted image pixels from a central server to a PCoIP device.

Pie chart

This ExtraHop chart displays metric data as a portion or percentage of a whole.

POP3

POP3 (Post Office Protocol) is a standard application-level protocol that transfers email messages between a server and a client application over a TCP connection.

Port mirroring

Port mirroring occurs when a network switch sends a copy of network packets from one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

Record

Records are structured flow and transaction information about events on your network. After you link an ExtraHop Discover appliance to an ExtraHop Explore appliance, you can generate and send records to the Explore appliance for storage and retrieval.

Region

A region is a dashboard component that contains widgets.

Retransmission Timeouts

Retransmission timeouts (RTOs) is a TCP protocol metric for determining network performance. TCP retransmissions occur on the network frequently. TCP starts a retransmission timer when an outbound segment is handed down to an IP address. If there is no acknowledgment (ACK) before the timer expires, the segment is retransmitted. An RTO occurs when the sender begins missing too many acknowledgments and stops sending segments for a period of time. RTOs can represent a 1-5 second delay on your network. Multiple RTOs over time can represents significant delays on your network.

Read the ExtraHop blog post: TCP RTOs: Retransmission Timeouts & Application Performance Degradation.

RPC

RPC (Microsoft Remote Procedure Call) is a communication mechanism for clients to call a procedure from a program located on another computer, server, or network.

RSPAN

Remote Switched Port Analyzer (RSPAN) provides remote monitoring of multiple switches across a switched network. RSPAN is a way to get traffic from a SPAN source on one switch to a SPAN destination on another switch that is connected via a trunk.

Note: RSPAN requires that the source and destination chassis are in the same Layer 2 domain.

RTCP

RTCP (Real-time Transport Control Protocol) is a protocol that monitors statistics for streaming audio and video data transferred by the RTP protocol.

RTP

RTP (Real-time Transport) is a protocol that defines the standardized packet format for the real-time transfer of streaming audio and video.

Sampleset metric type

In the ExtraHop system, this top-level metric type represents a summary of data that provides a mean (average) and standard deviation over a specified time period. Sampleset metrics typically summarize data about a detail metric.

Server

A server is a hardware system dedicated to hosting one or more services for users or clients on the network. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener.

SIP

SIP (Session Initiation Protocol) is a signaling protocol that controls communication sessions, such as voice calls for IP-based telephony applications.

SMPP

SMPP (short messaging peer-to-peer) is an application-level protocol that transfers Short Message Service (SMS) data between External Short Messaging Entities (ESME) and Short Message Service Centers (SMSC).

SMTP

SMTP (Simple Mail Transfer Protocol) is a standard protocol that sends, receives, and relays email messages between servers, email transfer agents, and client applications.

Snapshot metric type

In the ExtraHop system, this top-level metric type represents a data point that represents a single point in time. Snapshot metrics include ratios, current connections, and established TCP connections.

Source

In the ExtraHop system, a source provides access to collections of metrics. A source is an application, device (including device groups), or network (including VLANs).

SPAN

Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyzer (SPAN). SPAN copies traffic and sends it to a destination for network analysis.

SSL

SSL (Secure Sockets Layer) is a standard protocol for securing communication over the Internet. To establish an encrypted link between a web browser and a server, the server must have an SSL certificate.

Status chart

This ExtraHop chart type displays metric values in a column chart, where the color of the columns represents the status and severity of an alert assigned to the source and metric selected in the chart.

Telnet

Telnet is an application-layer protocol for interactive text-oriented communications over a virtual terminal connection.

Time Selector

The Time Selector is a tool that enables you to specify a time interval for the collection and presentation of network data in the ExtraHop Web UI. There are two types of Time Selectors: a Global Time Selector for specifying global time intervals and a Region Time Selector for specifying region time intervals in a dashboard.

Tinygram

A tinygram is a small packet or TCP segment. A tinygram is a packet where the payload is smaller than the frame header (L2-L4) data. In general, tinygrams lead to inefficient ratios of frame header data to actual useful information going across the network. Tinygrams can contribute to network congestion.

Read the ExtraHop blog post: What is a Tinygram?

Top-level metric

A top-level, or base, metric gives you a sum of data for a specified time period. Top-level metrics provide you with a big-picture value to help identify what is happening on your network. You can then drill down on a top-level metric to view detail metrics. There are different types of top-level metrics that provide different information, which include count, dataset, maximum, sampleset, and snapshot metric types. Understanding metrics types is essential to writing triggers and configuring charts.

Trigger

Triggers are custom scripts that perform an action upon a pre-defined event. For example, you can write a trigger to record a custom metric every time an HTTP request occurs, or to classify traffic for a particular server as an application server. For more information, see the Trigger API Reference.

Value chart

This ExtraHop chart displays the total value for one or more metrics. Selecting more than one metric will display the metric values side-by-side.

Virtual packet loss

Virtual packet loss (VPL) refers to a phenomenon that affects fully or partially virtualized applications. VPL creates symptoms that suggests network congestion and is often undetected by traditional network monitoring and application performance management (APM) tools. VPL occurs when a hypervisor schedules CPU time for an excessive number of virtual machines (VMs) and prevents those VMs from responding fast enough to TCP acknowledgements. VPL can be detected by a combination of application awareness and advanced TCP analysis.

VLAN

A Virtual Local Area Network (VLAN) is a logical grouping of traffic or devices on a network. VLAN information is extracted from VLAN tags, if the traffic mirroring process preserves the tags on the mirror port.

Widget

Widgets are configurable dashboard components that can be added to a region for different functions. Widget types are chart, text box, alert history, activity groups, and networks (Command appliance only).

Wire data

Wire data is created when data in flight is analyzed as traffic is sent over the network. Through real-time full-stream processing, unstructured data is reassembled into structured wire data that can be analyzed in real time. Wire data encompasses L2-L7 data that spans the entire application delivery chain and provides the most comprehensive, wide-reaching visibility.