ExtraHop Glossary

Published: 2018-07-07

AAA

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

ActiveMQ

ActiveMQ is an open-source, message broker from Apache.

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.

Activity maps

An activity map is a dynamic visual representation of the L4-L7 protocol activity between devices in your network. You can view real-time information about which devices and services are talking to each other across your network.

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.

Anomalies

Metric activity that deviates from what is standard, normal, or expected. Anomalies are detected by the ExtraHop Addy service.

AMF

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

AppFlow

The AppFlow protocol was developed by Citrix. This protocol is an extension of the IPFIX standard for monitoring network traffic. You can collect AppFlow traffic with the ExtraHop NetFlow module.

Application

In the ExtraHop system, applications are user-defined containers 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. In the ExtraHop system, you can create a basic application through the Web UI or an advanced application 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.

Atlas Remote Analysis

Through this service, ExtraHop analysts can perform an unbiased analysis of your network data and report on areas in your IT infrastructure where improvements can be made.

Audit log

The audit log on the Discover appliance provides data about the operations of the system, broken down by component. For example, when you log into an ExtraHop appliance, the successful or failed event is logged as an entry to the audit log.

Bar chart

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

Boxplot chart

The box plot chart displays variability for a distribution of metric data. Each box plot includes three or five data points. With five data points, the box plot contains a box, upper and lower whisker lines, and a tick mark. With three data points, the line contains upper and lower whisker lines, and a tick mark.

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.

Cluster

A group of the same ExtraHop appliances that are joined together.

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 of connected ExtraHop Discover appliances. The ECA provides a single view of data collected from multiple ExtraHop Discover, Explore, and Trace appliances, which can be distributed across data centers, branch offices, and the public cloud.

CORS

Cross-origin resource sharing (CORS) allows you to access the ExtraHop REST API across domain-boundaries and from specified web pages without requiring the request to travel through a proxy server. You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin. Only administrative users can view and edit CORS settings.

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

A dashboard is a customizable HTML page that displays different views of your network through widgets such as charts. In addition to custom dashboards, there are two built-in system dashboards that provide charts: the Activity dashboard and the Network dashboard.

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.

Deduplication

The ExtraHop system removes duplicate L2 and L3 frames and packets when metrics are collected and aggregated from your network activity by default. L2 deduplication removes identical Ethernet frames (where the Ethernet header and the entire IP packet must match); L3 deduplication removes TCP or UDP packets with identical IP ID fields on the same flow (where only the IP packet must match).

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. EDAs can be connected to the ExtraHop Command appliance for centralized management and connected to ExtraHop Trace and Explore appliances for data collection and querying.

Distinct count metric type

In the ExtraHop system, this top-level metric type represents 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.

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.

Dynamic baselines

Dynamic baselines are trend lines on dashboards that help you distinguish between normal and abnormal activity. Discover appliances calculate dynamic baselines based on historical data. To generate data points on a dynamic baseline, an appliance calculates the median value for a specified period of time.

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.

Event

An event represents activity detected from your network or from your ExtraHop system. Triggers can be written to collect the data associated with an event to create custom metrics.

Explore appliance

The ExtraHop Explore appliance (EXA) connects to 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.

Fingerprint

A fingerprint is a unique, alphanumeric identifier assigned to all Explore and Trace appliances.

FIX

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

Flow

A flow is a set of packets that are part of a single transaction between two endpoints. Similar to how the ExtraHop system can identify flows from wire data, flows from machine data on remote networks can be sent to a Discover appliance for analysis. Flows are identified through their unique combination of IP protocol (TCP/UDP), source and destination IP addresses, and source and destination ports. This combination is called a 5-tuple.

Flow interface

A flow network device can have multiple interfaces. Instead of looking at flow information for the entire device, you can look at flow information for a specific interface on the device.

Flow network

A flow network is a network device that sends information about flows seen across the device. Similar to how the ExtraHop system can identify flows from wire data, the ExtraHop system can receive flow information from remote network devices, also called flow exporters.

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.

ICMP

The Internet Control Message Protocol (ICMP) is a protocol that network devices send error and query messages through.

iDRAC

The Integrated Dell Remote Access Controller (iDRAC) provides remote access to ExtraHop appliances. After you enable and configure iDRAC, you can power cycle the system, view console messages, and review hardware monitoring and boot logs.

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).

Kerberos

Kerberos is a network authentication protocol for client and server applications that applies secret-key cryptography.

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?

Level-triggered alerts

A level-triggered alert is generated at specified intervals for as long as the metric value remains above the configured threshold.

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 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.

LLDP

The Link Layer Discovery Protocol (LLDP) is a protocol that network devices communicate their identity and capabilities through.

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.

MSMQ

Microsoft Message Queuing (MSMQ) is a protocol that enables applications to send messages and objects to each other.

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.

NetFlow

The NetFlow protocol was developed by Cisco for monitoring network traffic. You can send NetFlow traffic to the ExtraHop Discover appliance from remote flow networks to analyze data that is outside of your wire data feed.

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.

Network bytes

A network byte is a metric that displays the throughput rate of the ExtraHop capture process.

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

An indiviudal ExtraHop appliance within a cluster.

Open Data Stream

The open data stream (ODS) service enables you to send wire data to a remote third-party system, such as MongoDB or Kafka. You must write a trigger to identify and collect the data you want to export and configure settings in the ExtraHop Admin UI.

Packets

The Packets feature enables you to search for and download packets for selected transactions through a Discover or Command appliance. This feature requires an ExtraHop Trace appliance.

Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) is an encryption method that enables short-term, completely private key exchanges between clients and servers. You can license a Discover appliance to decrypt PFS SSL/TLS sessions from Windows servers where the ExtraHop PFS agent software is installed. Without PFS, those sessions could not be decrypted, and the data from those exchanges would be obscured.

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.

Protocol

A protocol defines the format and the order of messages exchanged between two or more devices, as well as the actions taken on the transmission and receipt of a message or other event.

Protocol page

A protocol page is a built-in page in the ExtraHop Web UI. You can access a protocol page in the by logging into the Web UI, clicking **Metrics**, and then clicking the name of a source or group; all protocol pages for the source or group are listed in the left column.

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.

Record format

A record format is a schema on read that determines how each record displays in the Web UI. The Discover and Command appliances have built-in record formats for all built-in record types, and although you cannot modify a built-in record format, you can create a custom record format.

Record types

Record types link the records that are indexed and stored in the Explore appliance with the record format in the Web UI.

Redis

Redis is an open-source, data structure server.

Region

A region is a dashboard component that contains widgets.

Retransmission Timeout (RTO)

A retransmission timeout (RTO) 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 represent 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.

Remote packet capture (RPCAP)

Remote packet capture (RPCAP) is a software implementation for packet forwarding that is similar to a physical tap. If you want to monitor network traffic for devices that are not directly connected to your wire data feed, you can forward packets through the cloud and analyze that data through the ExtraHop Discover appliance.

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.

Runtime Log

The runtime log is a component of the Trigger Editor in the ExtraHop Web UI. The runtime log displays exceptions and output from debug statements in trigger scripts.

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.

SDP

The Session Description Protocol (SDP) is a protocol that defines multimedia streaming sessions.

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.

SNMP

The Simple Network Management Protocol (SNMP) is a layer-7 protocol for collecting, organizing, exchanging, and modifying information about managed devices on IP networks.

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.

SSH

Secure Shell (SSH) is a protocol that securely transmits information over a network.

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.

Table chart

This ExtraHop chart type displays metric values across rows and columns in a table.

TCP

In the ExtraHop system, TCP (Transmission Control Protocol) metrics provide information about the reliable transfer of packets between a source and destination. Through TCP metrics, ExtraHop provides visibility into which devices are connected to each other, when devices send data, if there are errors in the data, what protocols are communicated through, and so on.

TCP RST

A TCP RST packet is sent to prevent a TCP connection from being established or to forcibly terminate an existing connection. Sometimes resets are sent when the receiving device failed to ACK the SYN packet, or it failed to acknowledge another packet sent and retransmitted later in the transaction. In some cases, TRCP RSTs indicates that an error occurred. High volumes of outbound resets should be investigated to determine if they are expected behavior or indicative of a larger issue.

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.

Timestamp

A timestamp is a digital record of the time a particular event occurred. In the ExtraHop system, you can select the default timestamp, or configure external timestamps such as Gigamon or Anue through the Running Configuration file.

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.

Topnset

A topnset is the top 1,000 key-value pairs calculated for the time interval you specify in the Time Selector. A topnset is not a complete data set because a topnset only represents the key-values that are recorded for a specific aggregation roll up (based on a specified time interval), and is limited to up to 1,000 keys per topnset.

Trace appliance

The ExtraHop Trace appliance (ETA) continuously collects network packets and connects to the ExtraHop Discover appliance to enable you to quickly retrieve all packets that match a set of search criteria within a given time interval.

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.

Trouble groups

A trouble group is a collection of devices that are exhibiting some form of potentially problematic behavior, such as aborted HTTP or database transactions.

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.