Explore metrics in the ExtraHop system to investigate DNS failures

Published: 2020-02-23

The DNS (domain name system) protocol is critical for supporting internet traffic. It often works without issues. However, DNS servers are commonly misconfigured or overloaded in IT environments, which can affect internet performance.

There are many ways to explore DNS metrics in the ExtraHop system. In this walkthrough, we'll show you how to review DNS metrics in a dashboard, navigate to DNS protocol pages, and drill-down on interesting metrics to identify potentially-affected devices.

Specifically, you'll learn how to answer the following questions:

- Is there a network or DNS issue that is affecting internet performance?
- What are the number of DNS failures on my network?
- Which clients are affected by DNS issues?

Additional resources are available for interpreting DNS:

- Learn about interpreting DNS metrics in the ExtraHop system by viewing our online training module, Quick Peek: DNS.
- Learn about problem DNS queries and errors that you can monitor in your own environment by installing the ExtraHop DNS Bundle. This bundle contains a dashboard with pre-configured charts and detailed explanations about key DNS errors.
- Learn how to build a dashboard to monitor DNS errors.

Prerequisites

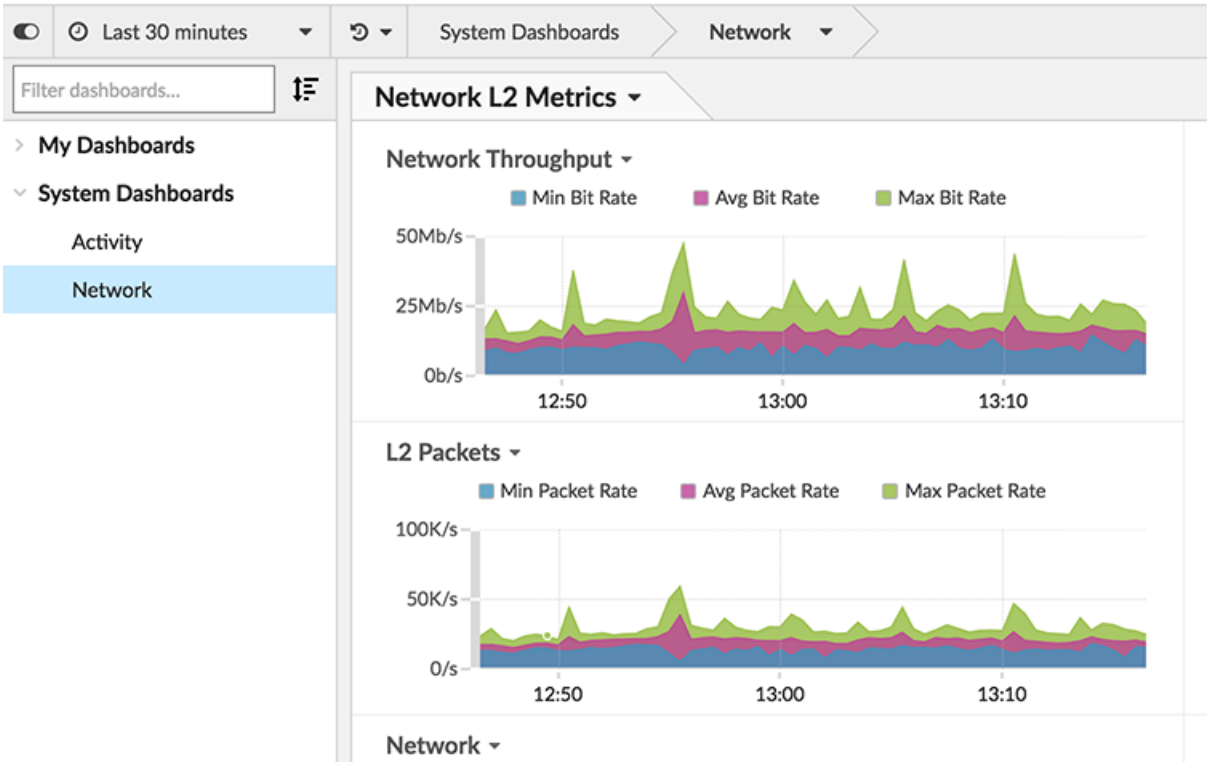
- Familiarize yourself with the concepts in this walkthrough by reading the Metrics topic.
- You must have access to an ExtraHop Discover appliance with DNS server traffic, or you can perform this walkthrough in the ExtraHop demo.

Identify DNS issues with system dashboards

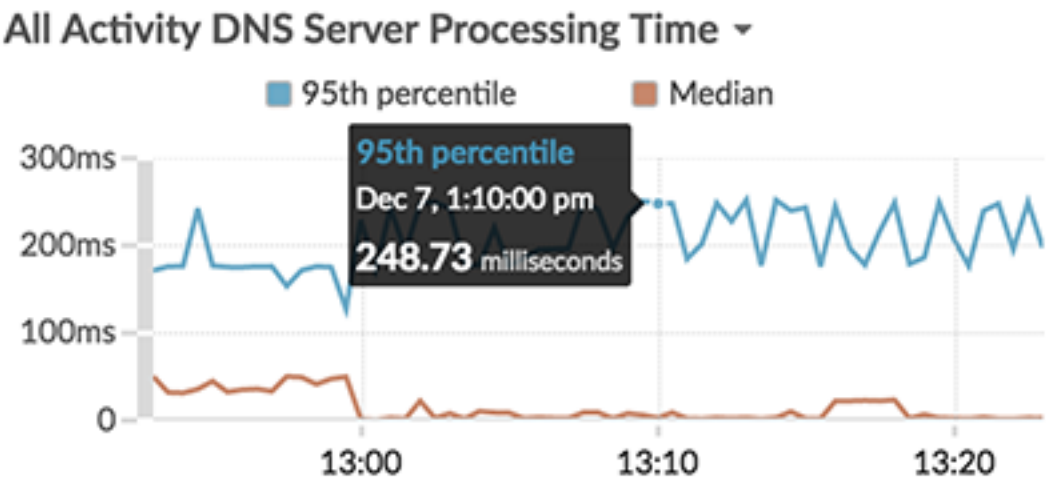
If a slow internet issue is reported, look at the system dashboards to determine whether the issue is related to network throughput or to the DNS protocol.

1. Log into the Web UI on the Discover appliance.
2. Click **Last 30 minutes** in the top-left navigation bar, select **Last week**, and then click **Save**.

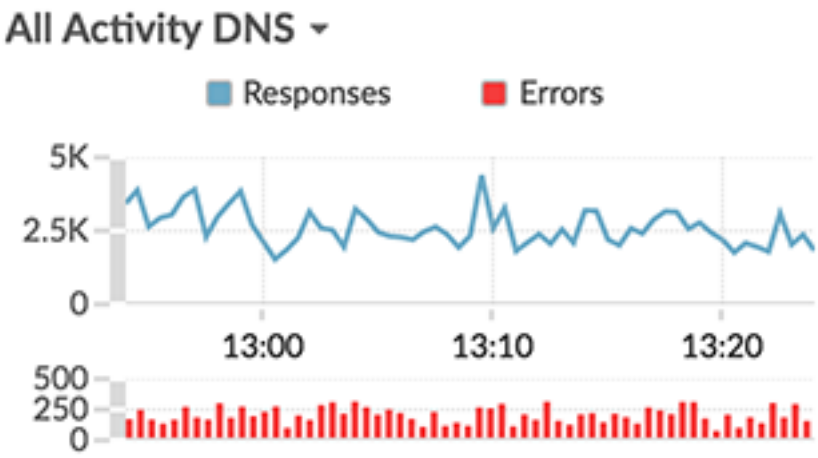
   Note: Changing the global time interval gives you a chance to see network and protocol behavior that occurred prior to the detected problem.
3. Click **Dashboards**, and then click **Network** in the System Dashboards collection.
4. Confirm that the Network Throughput and L2 Packets charts show normal or consistent peaks, similar to the figure below. A large discrepancy between maximum rates and average rates can indicate network issues are affecting internet performance. Otherwise, continue your investigation into DNS metrics.



5. Click **Activity** in the System Dashboards collection.
6. Scroll down to the All Activity DNS Server Processing Time and All Activity DNS charts.
   a) The All Activity DNS Server Processing Time chart shows you the time between the last packet of a DNS request from a client and the first packet of a DNS response from the server. Hover over the median to compare the processing time at the same time point. A large difference between the median value and 95th percentile indicates that something might be wrong with a DNS server in your network.



   b) The All Activity DNS chart correlates responses and errors. A spike in errors can add delays of two to four seconds for clients, servers, applications, and customers. In the figure below, the proportion of responses to errors looks consistent.



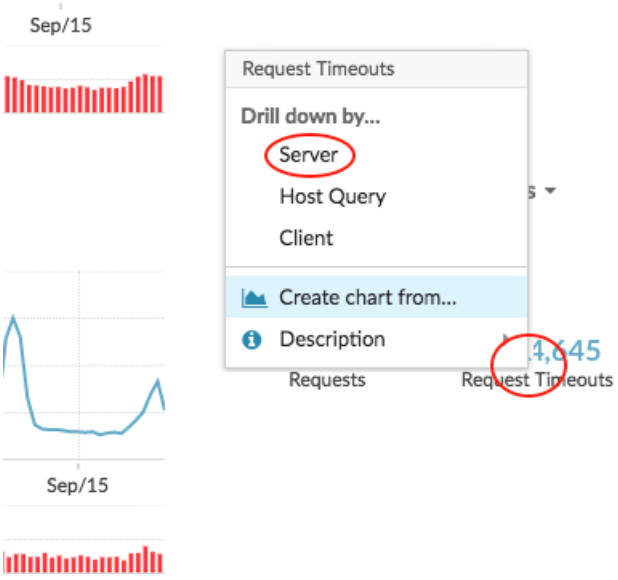
Based on these dashboard charts, the network throughput appears okay but DNS server processing time seems unusual. Next, we should investigate more DNS server metrics to pinpoint the cause of the slowdown.

View the number of DNS Request Timeouts

The DNS metric, Request Timeouts, indicates a failure to fulfill a DNS request. DNS servers that are not fulfilling requests can negatively affect application and internet performance. Let's look at the total number of Request Timeouts for DNS servers on our network on a protocol page. The protocol page for the All Activity application provides an overview of important metrics for all the activity across your network, including DNS protocol activity. We can then drill-down to see which DNS servers are timing out.

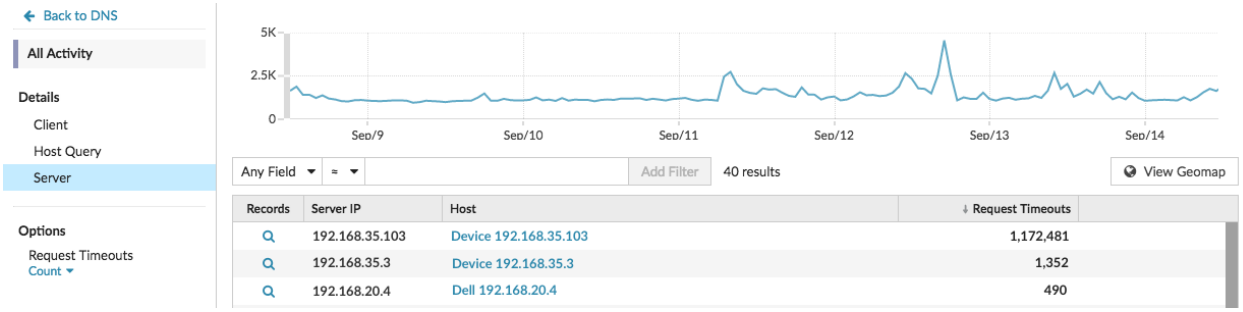
1. On the Activity dashboard, click the **All Activity DNS** chart title.
2. In the Go to application... section of the drop-down menu, click **All Activity DNS**.
   The All Activity protocol page appears.
3. In the left pane, click **DNS**.
4. View the number of Request Timeouts. In the figure below, the number is high (1,174,645) and worth investigating further.

5. Click the metric value for Request Timeouts and then select **Server**, as shown in the figure below.



A detail metric page appears that displays all the server IP addresses in your network with request timeouts.

6. Note which devices have the highest number of Request Timeouts. In the figure below, this is Device 192.168.35.103.

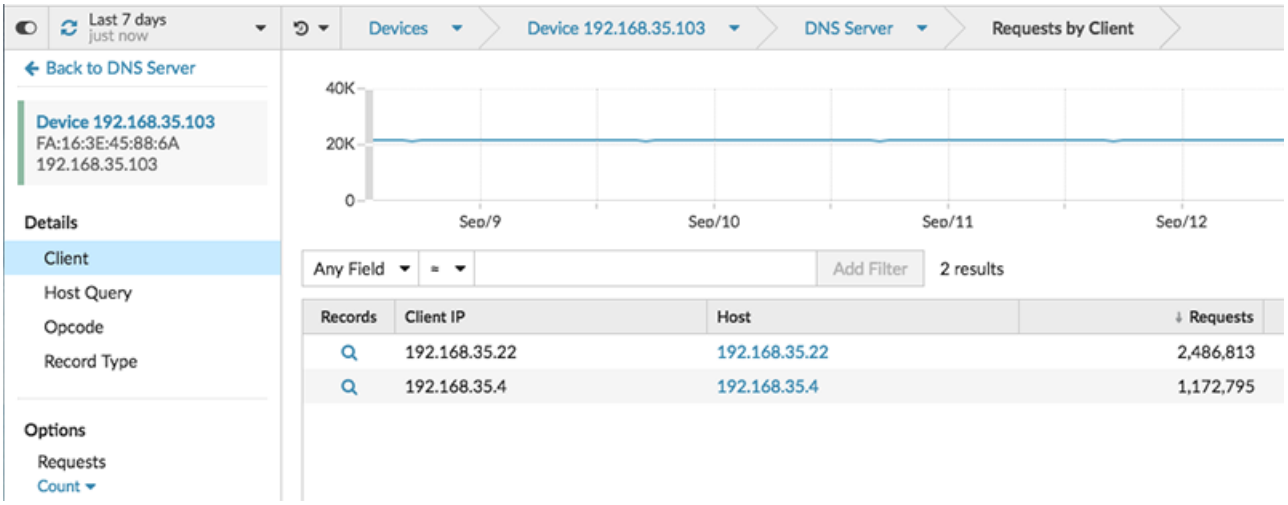


7. In the Host column, click the name of the device with the highest number of request timeouts.
A new protocol page appears, which displays metrics specific to Device 192.168.35.103. Now we can examine which clients are affected by this DNS server.

Find the clients affected by DNS Request Timeouts

You can now identify which clients sent requests to this DNS server and might be affected by DNS Request Timeouts.

1. From the protocol page for Device 192.168.35.103, click **DNS** in the Server Activity section in the left pane.
2. In the DRILL DOWN section near the top of the page, click **Clients**.



A detail metric page appears that displays all the client IP addresses that sent requests to the DNS server.

Next steps

From this detail metric page, you can also learn about which host queries and record types were included in the requests by selecting an option in the Details section of the left pane. Or, investigate related metrics for each client by clicking the link in the Host column.

Based on the data you gathered, you can now contact the team responsible for maintaining this specific DNS server, because it might be misconfigured or experiencing other issues.