Investigate detections

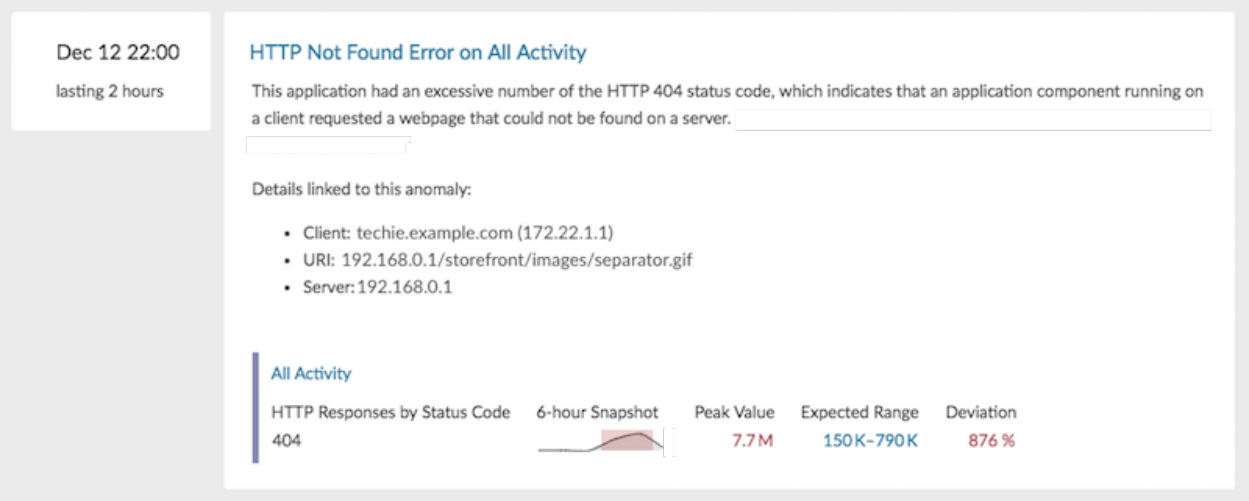
Published: 2020-02-22

Automated investigation is available for most detections. By viewing detail metrics in the detection description, you can immediately learn which factors contributed to an issue. When multiple factors contribute to an detection, you can also see the percentage of their contribution to the detection.

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

Note: Automated investigation is not available for server processing time detections. For these detections, you can investigate detections from a protocol page in the Discover or Command appliance.

For example, the following figure shows which client, server, and URI are linked to an HTTP 404 detection.

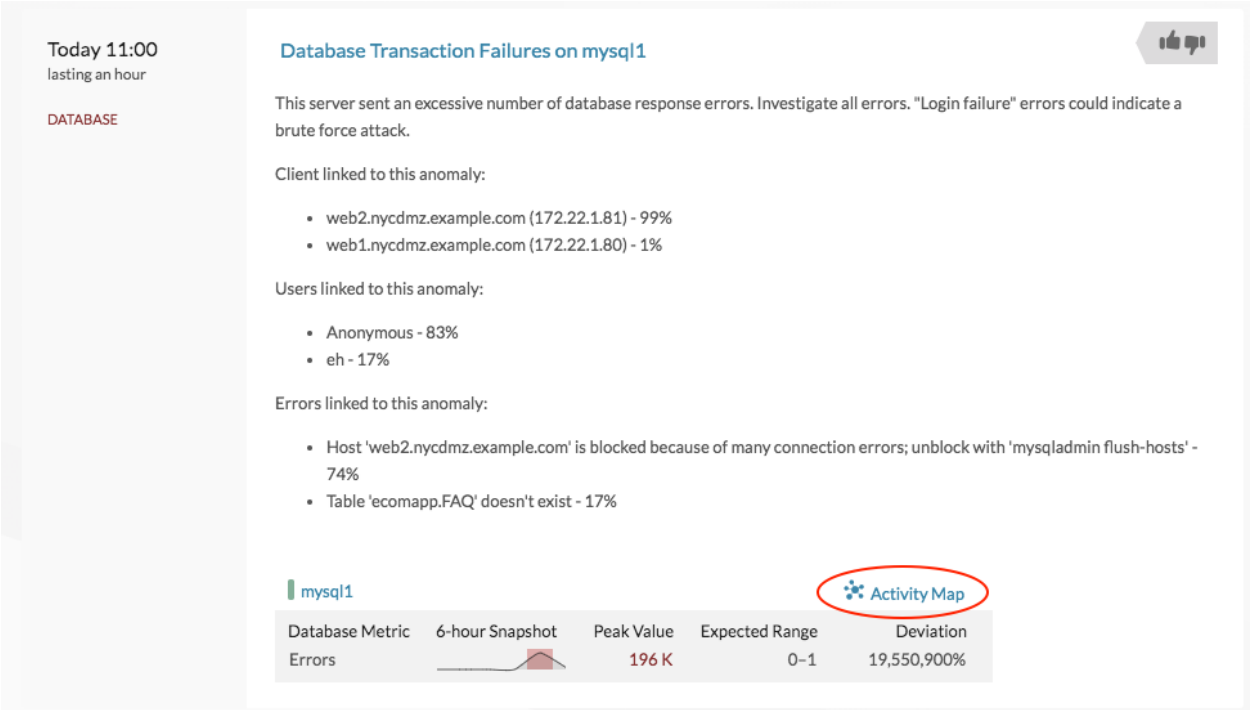


To learn more about the scope of a detection on your network, you can continue your investigation by opening an activity map or visiting a protocol page.

Open an activity map from a detection

When a single client or server is associated with unusual L7 protocol activity, such as a high number of HTTP errors or DNS request timeouts, an activity map link appears.

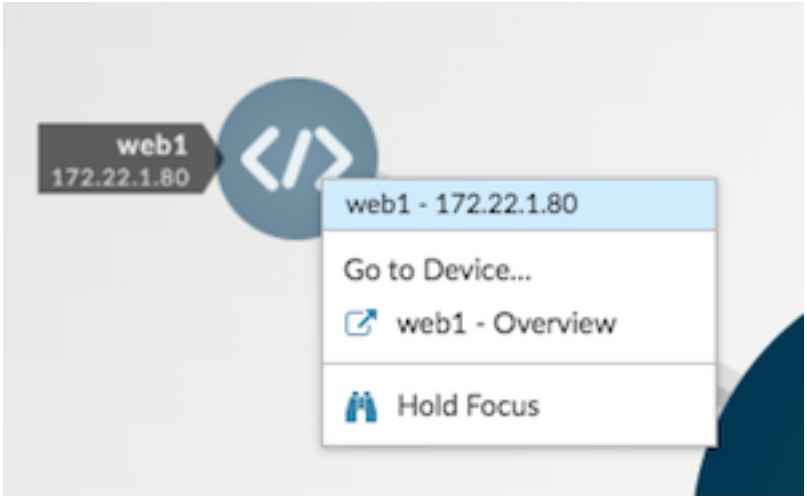
1. Log into the Web UI on a Discover or Command appliance, and then click **Detections** at the top of the page.
2. Find the detection that you want to investigate. The following figure shows an example of the **Activity Map** link for a database server that sent an unusual number of errors.



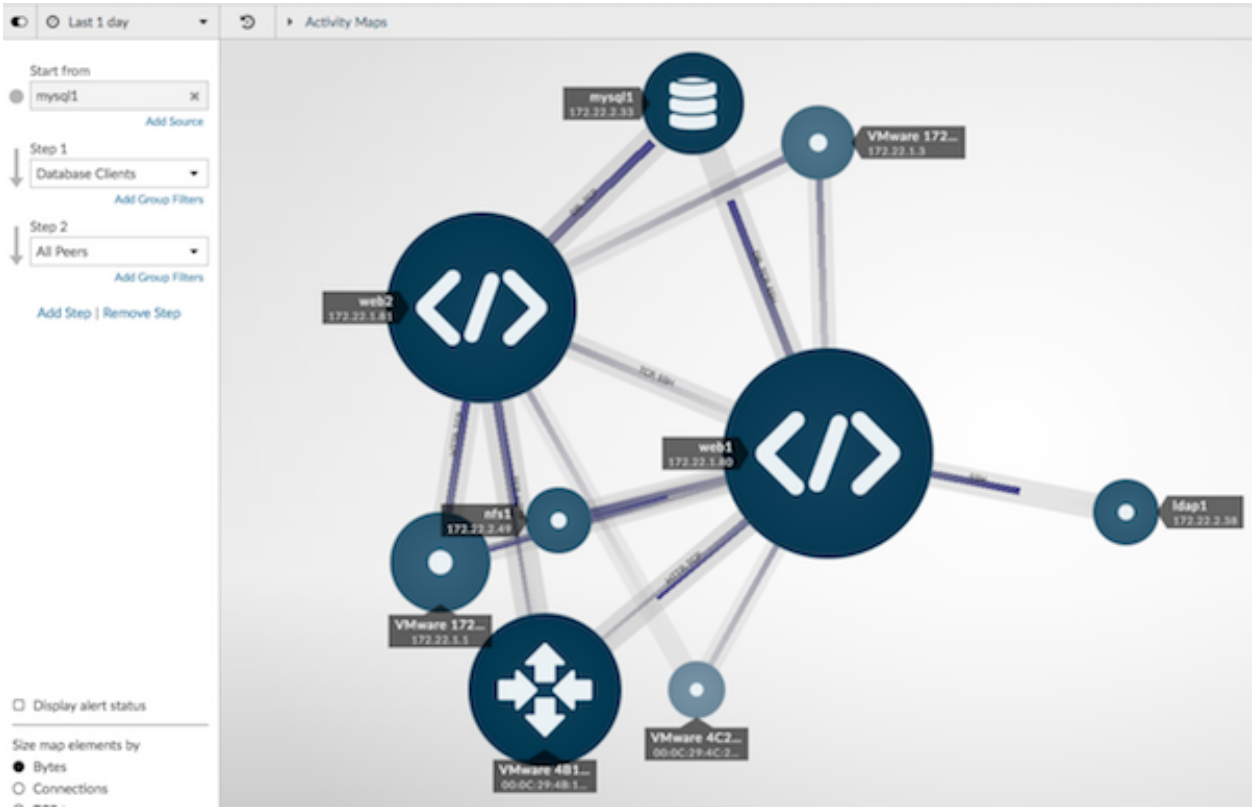
3. Click **Activity Map**.
   An activity map appears for the database server. The activity map in the following figure shows the two database clients that were connected to the server during the detection time frame.

You can now interact with the activity map to learn more about the effect of the database errors across the network:

- Click any client in the map to access a menu that contains a Go to Device... link. Click the link to open a protocol page with client metrics, such as requests and responses.



- In the left pane below Step 1, click **Add Step** and then click **All Peers** in the drop-down list. The map updates to show you which downstream devices are connected to the database clients, as shown in the following figure.



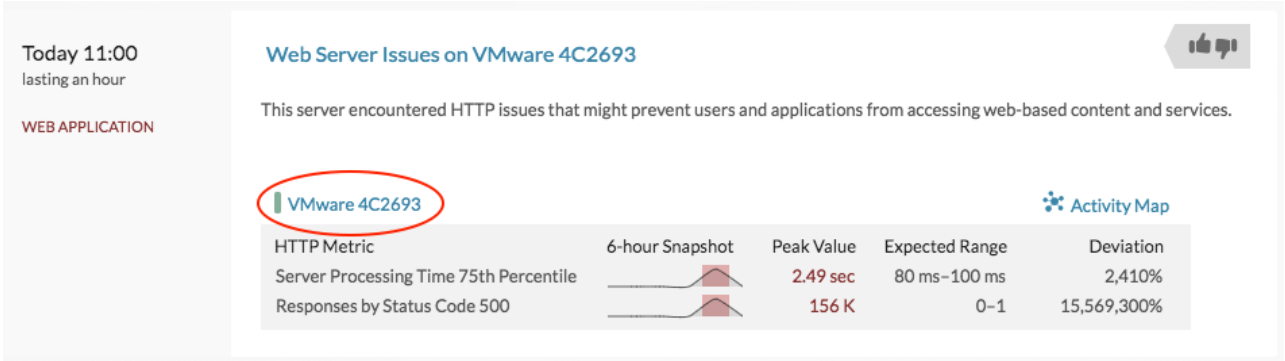
- Save and then share your activity map with other ExtraHop users.

For more information about activity maps, see Activity maps.

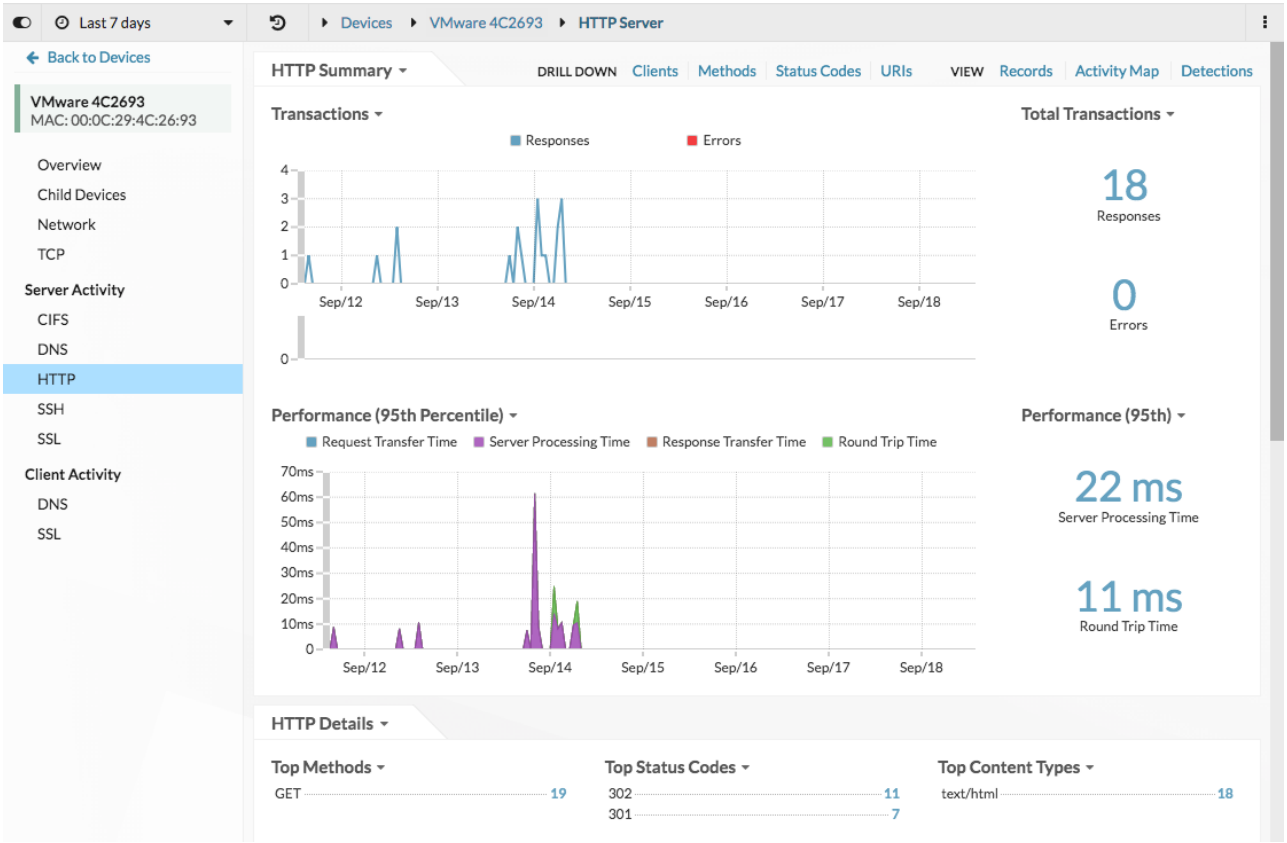
Navigate to a protocol page

If you want to further investigate anomalous metrics, you can navigate to a protocol page where you have access to additional charts, metrics, and tools.

1. Log into the Web UI on a Discover or Command appliance, and then click **Detections** at the top of the page.
2. Find the detection that you want to investigate.
3. Click the source name, as shown in the following figure.



The anomalous protocol page for the device or application appears, which displays all of the metric data associated with that specific device or application during the detection time interval, as shown in the figure below.



Next steps

From a protocol page, you can then choose one of the following options to further investigate metric data:

- Create an activity map
- Drill down on metrics

Best practices for investigating detections

The Machine Learning Service provides you with high-quality, actionable data about detections—but does not replace decision-making or expertise about your network. The following best practices explain how to determine which detections are worth further investigation and when to take action.

Change the time interval to see when detections occurred

Learn if detections occurred before, after, or during a reported problem. For example, does the time frame of the detection coincide with a reported issue, such as slow load times or login times? You can also compare detections from the past month to the current date, which gives you a sense of whether the occurrence or severity of detections is changing over time.

For more information, see Filter the detections list.

Compare additional metrics or sources

Click the sparkline to open the Metric Explorer for the metric. Metric characteristics, such as the source, time interval, and drill-down details are preserved so that you can quickly create a chart from the metric or add additional sources and metrics for comparison.

Create a detection alert

You can configure an alert to receive email notifications when a detection occurs. Detection alerts also help you quickly find detections for a specific device or application on the Alert History page.

For more information, see Configure detection alert settings.

Filter detections by protocol

Filter by protocol to quickly monitor critical protocols with a role in security, commerce, or communication processes.

For example, an FTP 530 error detection might indicate that someone is trying to gain unauthorized access to information on your network. Or Citrix server and client latency detections might indicate that users are experiencing long load times for their roaming desktop profiles.

Selecting different protocols can also show you how detections correlate to each other. An anomalous HTTP response time followed immediately by an anomalous CIFS server processing time might suggest that web servers are dependent on how quickly your file storage servers can send and receive file data.

For more information, see Detections.