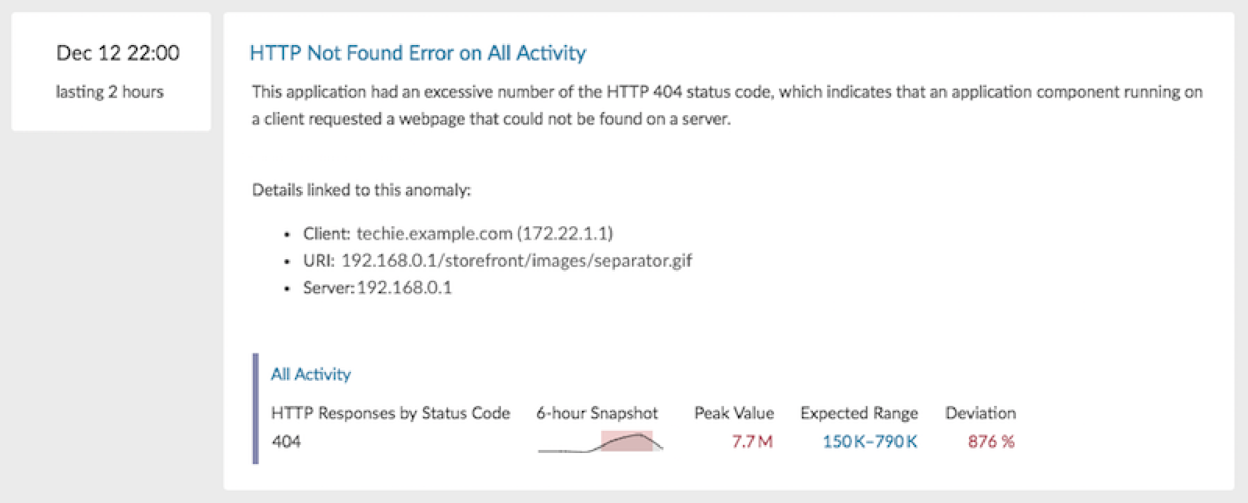
Investigate detections

Published: 2018-11-07

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



Dec 12 22:00

lasting 2 hours

HTTP Not Found Error on All Activity

This application had an excessive number of the HTTP 404 status code, which indicates that an application component running on a client requested a webpage that could not be found on a server.

Details linked to this anomaly:

- Client: techie.example.com (172.22.1.1)
- URI: 192.168.0.1/storefront/images/separator.gif
- Server:192.168.0.1

All Activity

HTTP Responses by Status Code	6-hour Snapshot	Peak Value	Expected Range	Deviation
404		7.7 M	150 K–790 K	876 %

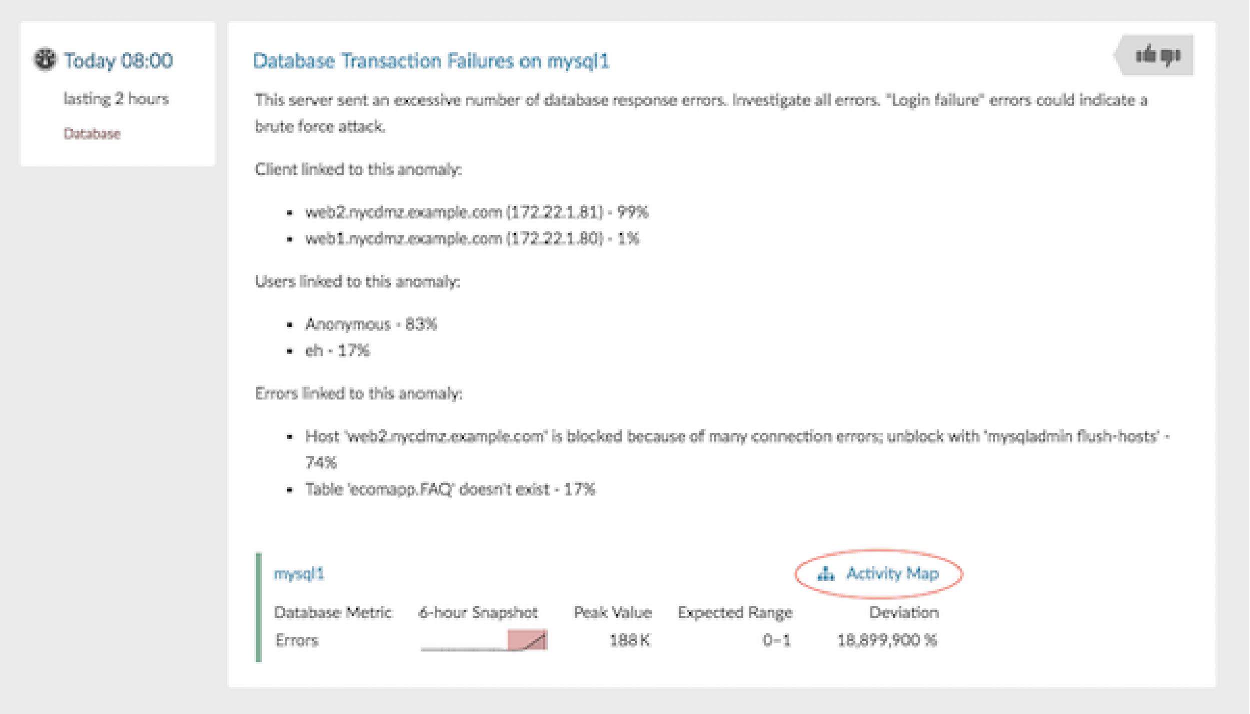
Note: Automated investigation is not available for server processing time detections. For these detections, you can investigate detections from a protocol page in the Discover or Command appliance.

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.



Today 08:00

lasting 2 hours

Database

Database Transaction Failures on mysql1

This server sent an excessive number of database response errors. Investigate all errors. "Login failure" errors could indicate a brute force attack.

Client linked to this anomaly:

- web2.nycdmz.example.com (172.22.1.81) - 99%
- web1.nycdmz.example.com (172.22.1.80) - 1%

Users linked to this anomaly:

- Anonymous - 83%
- eh - 17%

Errors linked to this anomaly:

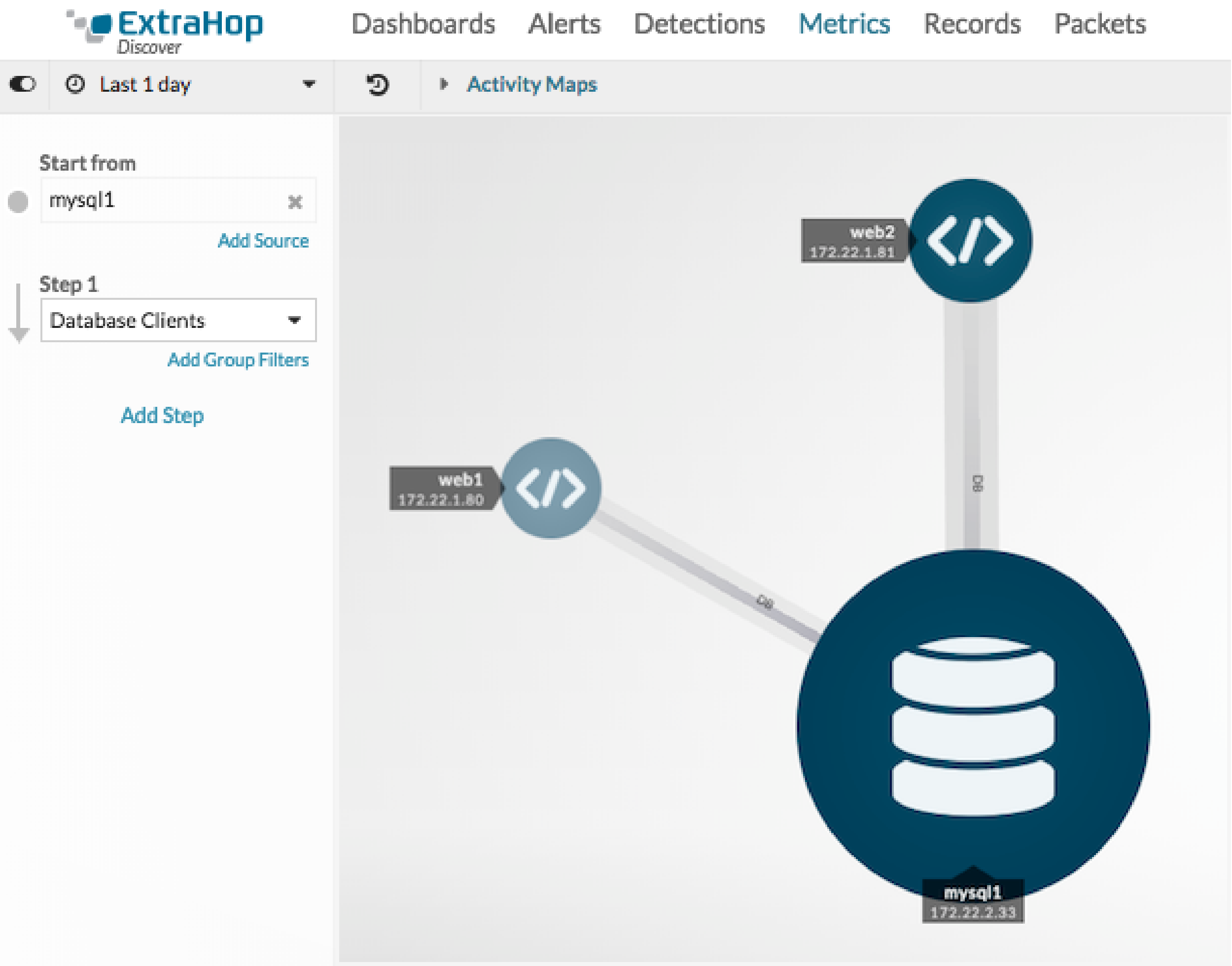
- Host 'web2.nycdmz.example.com' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts' - 74%
- Table 'ecomapp.FAQ' doesn't exist - 17%

mysql1

Activity Map

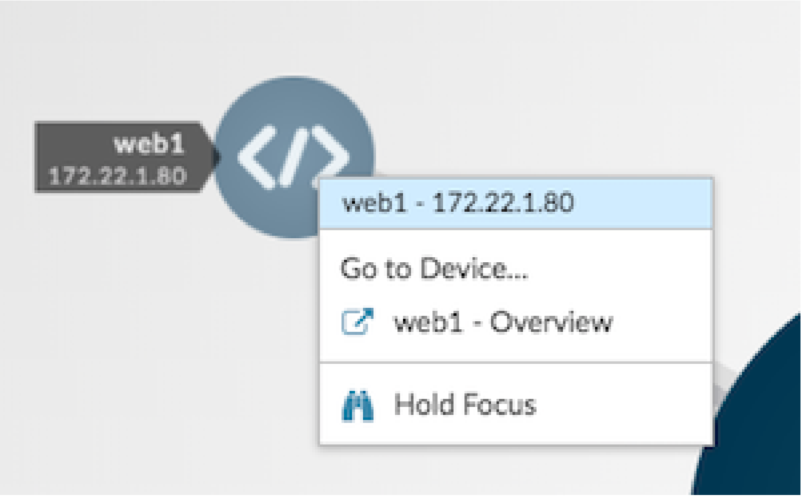
Database Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Errors		188 K	0–1	18,899,900 %

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.

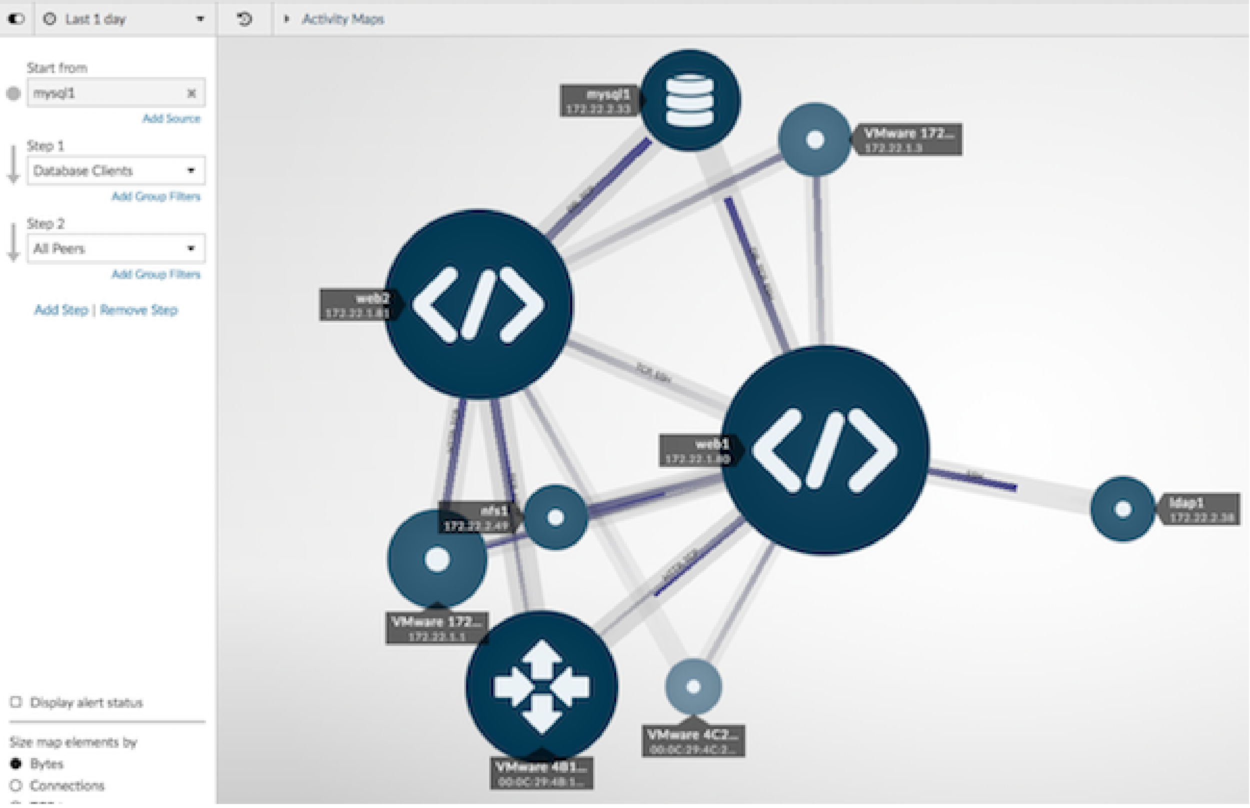


You can now interact with the activity map to learn more about the effect of the database errors across the network:

- 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.


Last 1 day

Activity Maps

Start from

mysql1

Add Source

Step 1

Database Clients

Add Group Filters

Step 2

All Peers

Add Group Filters

Add Step | Remove Step

☐ Display alert status

Size map elements by

● Bytes

○ Connections

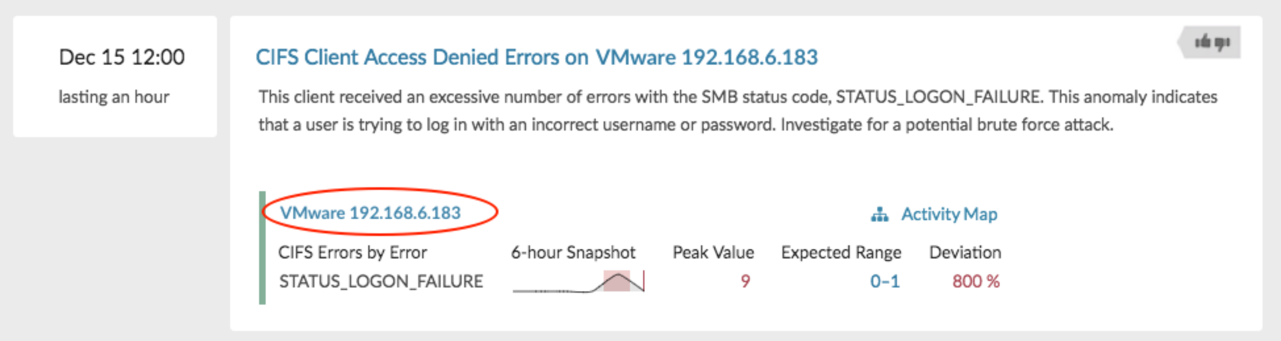
- Save and then share your activity map with other ExtraHop users.

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.



Dec 15 12:00

lasting an hour

CIFS Client Access Denied Errors on VMware 192.168.6.183

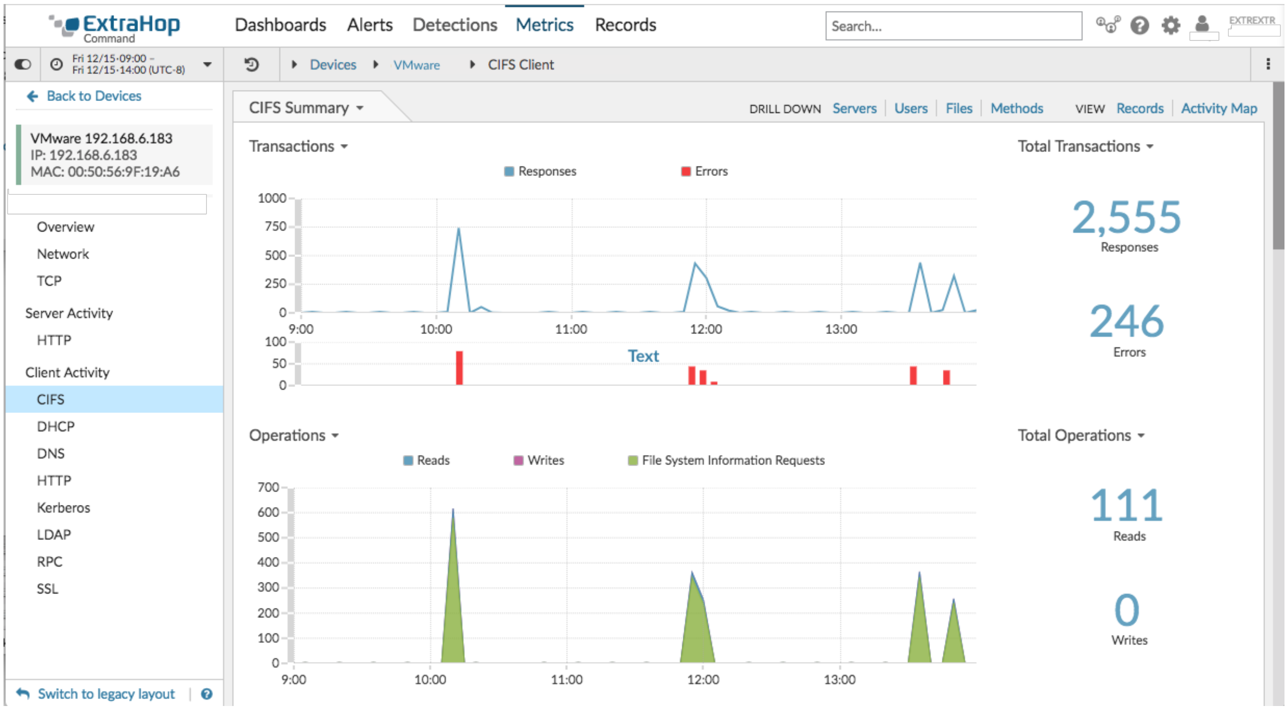
This client received an excessive number of errors with the SMB status code, STATUS_LOGON_FAILURE. This anomaly indicates that a user is trying to log in with an incorrect username or password. Investigate for a potential brute force attack.

VMware 192.168.6.183

Activity Map

CIFS Errors by Error	6-hour Snapshot	Peak Value	Expected Range	Deviation
STATUS_LOGON_FAILURE		9	0–1	800 %

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 Find and filter detections ↗.

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 Find and filter detections ↗.