

Investigate performance detections

Published: 2020-02-23

When an interesting detection appears, you should investigate whether the detected behavior points to a low-priority issue or to a potential problem. You can start your investigation directly from the detection card, which provides links to data across the ExtraHop system.

There are a number of [tools that can help you filter](#) your view to see the detections that you want to prioritize for investigation. Look for the following trends to get started:

- Did any detections occur at unusual or unexpected times, such as user-activity on weekends or after hours?
- Are any detections appearing in large clusters on the timeline?
- Are there detections appearing for critical assets or high-value endpoints?

Start your investigation

Review the detection title and summary to learn what caused the detection.

Database Transaction Failures on mysql1-nyc

16 171

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

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-nyc
172.22.2.33

[Activity Map](#) [Records](#)

Database Metric	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
Errors		196 K	0-1	19,550,900%

What caused this detection?

What should I investigate?

Refine your investigation

A detection card includes several links to data within the ExtraHop system. The availability of these links depends on which devices and metrics are associated with the detection. Each link is described in the sections below.

Device name

Click a device name to navigate to a protocol page, which contains all of the protocol metrics associated with the device. A protocol page gives you a complete picture of what this device was doing at the time of the detection. Click **Overview** in the left pane to see the role, users, and tags associated with that device.

For example, if you get a detection about database transaction failures, you can learn about other activity associated with the server hosting the database instance.

Today 11:00
lasting an hour

DATABASE

CLOSED
Action Taken

✓ OPER-7829

kpickles

Database Transaction Failures on mysql1.nycprod.example.com

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.nycprod.example.com

[Activity Map](#) [Records](#)

172.22.2.33

Database Metric	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
Errors		196 K	0-1	19,550,900%

Availability

Device name links are only available for devices that have been automatically discovered by the ExtraHop system. Remote devices that are located outside of your network are represented by their IP addresses.

Activity map

Click **Activity Map** to see device connections by protocol during the time of the detection. For example, if you get a detection about LDAP authentication errors, you can create an activity map to learn which devices were connected to an LDAP server during the detection.

Today 11:00
lasting an hour

AUTHORIZATION & ACCESS CONTROL

IN PROGRESS

● OPER-7831

kpickles

LDAP Server Auth Errors on ldap1-nyc

This server sent an excessive number of the LDAP invalidCredentials error.

Client linked to this anomaly:

- 172.29.1.101

ldap1-nyc

[Activity Map](#)

[Records](#)

172.22.2.38

LDAP Errors by Error Code	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
invalidCredentials		20.8 K	0-1	2,078,700%

Availability

An activity map is available 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.

Records

Click **Records** to navigate to a Records page, which includes structured information about client-server transactions within customizable fields. For example, if you get a detection about LDAP authentication errors, you can learn which methods and distinguished names contributed to the LDAP errors.

LDAP Server Auth Errors on ldap1-nyc

This server sent an excessive number of the LDAP invalidCredentials error.

Client linked to this anomaly:

- 172.29.1.101

ldap1-nyc
172.22.2.38

[Activity Map](#) [Records](#)

LDAP Errors by Error Code	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
invalidCredentials		20.8 K	0-1	2,078,700%

Availability

Records are available when you have a connected Explore appliance.

Detail metric drill down

Click a detail metric link to drill down on a metric value. A detail metric page appears, which lists metric values by a key, such as client IP address, server IP address, method, or error. For example, if you get an authentication detection about an LDAP server, drill down to learn which client IP addresses submitted the invalid credentials that contributed to the total number of LDAP errors.

LDAP Server Auth Errors on ldap1-nyc

This server sent an excessive number of the LDAP invalidCredentials error.

Client linked to this anomaly:

- 172.29.1.101

ldap1-nyc
172.22.2.38

[Activity Map](#) [Records](#)

LDAP Errors by Error Code	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
invalidCredentials		20.8 K	0-1	2,078,700%

Availability

The drill-down option is available for detections associated with topset detail metrics.

Sparkline

Click the sparkline to create a chart that includes the source, time interval, and drill-down details from the detection, which you can then add to a dashboard for additional monitoring. For example, if you get a detection about web server issues, you can create a chart with the 500 status codes sent by the web server and then add that chart to a dashboard about website performance.

Today 11:00
lasting an hour


WEB APPLICATION

NEW

- OPER-7830
- kpickles



Web Server Issues on VMware 4C2693 👍👎

This server encountered HTTP issues that might prevent users and applications from accessing web-based content and services.



VMware 4C2693
00:0C:29:4C:26:93

[Activity Map](#) [Records](#)

HTTP Metric	6-hour Snapshot	6-hour Peak Value	Expected Range	Deviation
Server Processing Time 75th Percentile		2.49 sec	80 ms-100 ms	2,410%
Responses by Status Code 500		156 K	0-1	15,569,300%

Availability

The sparkline option is available for detections that were associated with metrics and had a duration over one-hour. For 1-second metrics, a sparkline is available when the duration was over 30-seconds.

Investigate performance detections 4