

Investigate anomalies with Addy

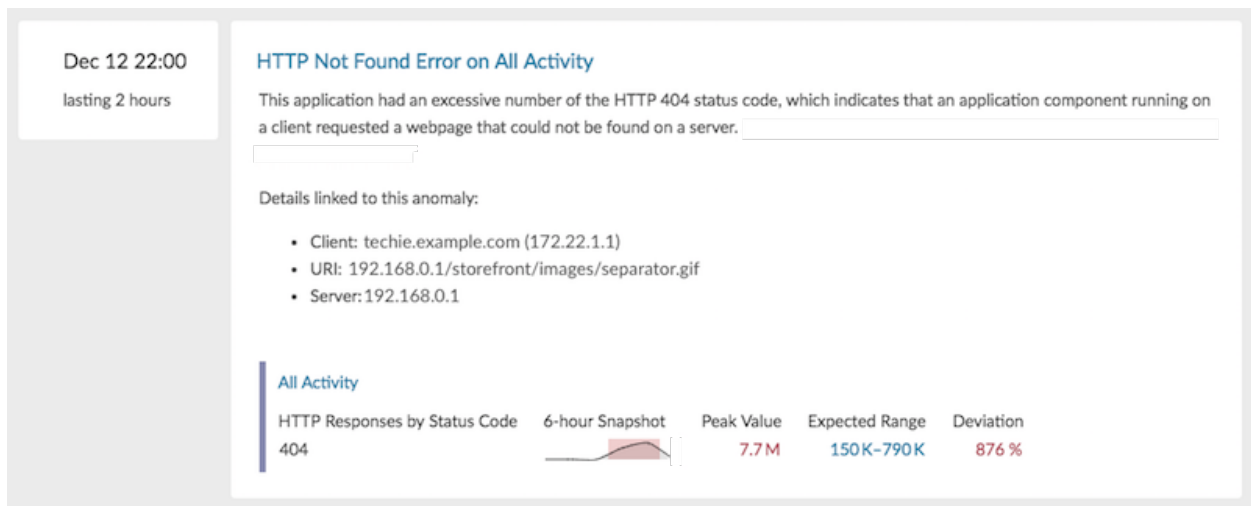
Published: 2018-01-11

When you find an interesting anomaly, you want to better understand the root cause. You can begin your investigation by reviewing information revealed by automated investigation or by navigating to a protocol page.

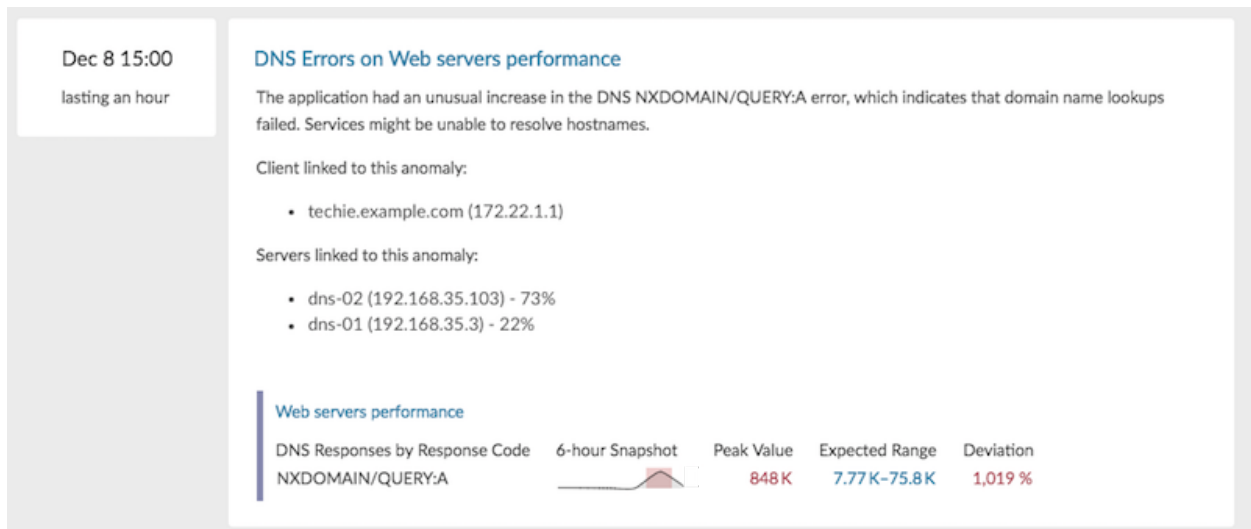
Addy automated investigation

Addy performs an automated investigation for most anomalies, which means that you can view detail metrics in the anomaly description to immediately learn what contributed to an issue.

In the following figure, you can see which client, server, and URI are linked to an HTTP 404 anomaly.



When multiple factors contribute to an anomaly, you can also see the percentage of their contribution to the anomaly. For example, the following figure shows the top two DNS servers that sent an excessive number of DNS errors to a client during the detected anomaly.



Note: Automated investigation is not available for server processing time anomalies. For these anomalies, you can [investigate anomalies from protocol pages in the Discover or Command appliance](#).

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 metrics and tools, such as activity maps.

1. Log into the Web UI on the Discover appliance and then click **Anomalies** at the top of the page.
2. Find the anomaly that you want to investigate.
3. Click the source name, as shown in the figure below.

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

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 anomaly time interval, as shown in the figure below.

ExtraHop Command

Dashboards Alerts Anomalies **Metrics** Records

Search...

Fri 12/15-09:00 - Fri 12/15-14:00 (UTC-8)

Devices > VMware > CIFS Client

Back to Devices

VMware 192.168.6.183
IP: 192.168.6.183
MAC: 00:50:56:9F:19:A6

Overview
Network
TCP
Server Activity
HTTP
Client Activity
CIFS
DHCP
DNS
HTTP
Kerberos
LDAP
RPC
SSL

Switch to legacy layout

CIFS Summary

DRILL DOWN Servers Users Files Methods VIEW Records Activity Map

Transactions

Responses Errors

1000
750
500
250
0
9:00 10:00 11:00 12:00 13:00

Text

100
50
0

Total Transactions

2,555 Responses
246 Errors

Operations

Reads Writes File System Information Requests



700
600
500
400
300
200
100
0
9:00 10:00 11:00 12:00 13:00

Total Operations

111 Reads
0 Writes

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 anomalies

Published: 2018-01-11

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

Change the time interval to see when anomalies occurred

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

For more information, see [Find and filter anomalies with the Addy service](#).

Create an anomaly alert

You can configure an alert to receive email notifications when an anomaly occurs. Anomaly alerts also help you quickly find anomalies for a specific device or application on the [Alert History](#) page.

For more information, see [Configure Addy anomaly alert settings](#).

Filter anomalies 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 anomaly might indicate that someone is trying to gain unauthorized access to information on your network. Or Citrix server and client latency anomalies might indicate that clinicians cannot access patient information in a timely fashion.

Selecting different protocols can also show you how anomalies 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 anomalies with the Addy service](#).