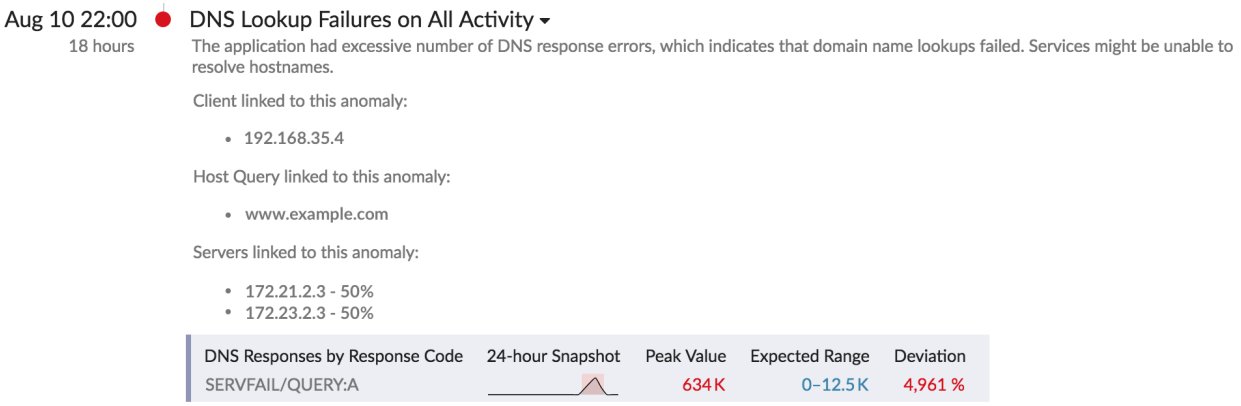
Investigate the root cause of anomalies with the Addy service

Published: 2020-02-22

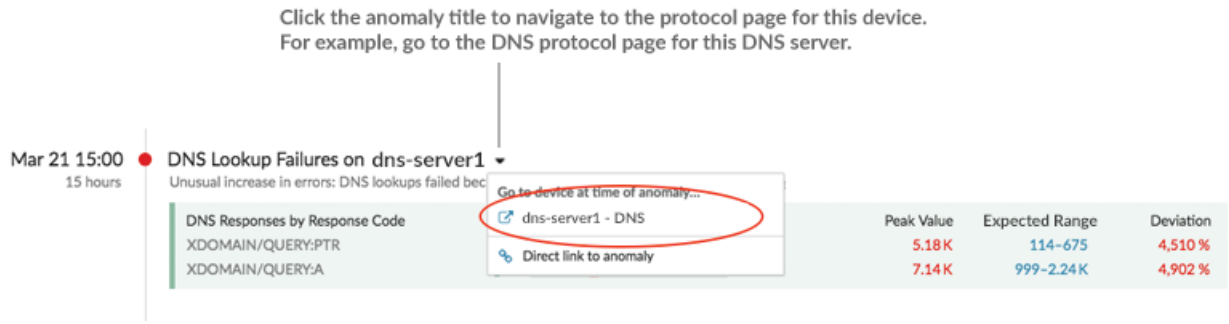
After connecting a Discover appliance to the ExtraHop Addy service for anomaly detection, you can begin searching for anomalies. For most anomalies, Addy performs an automated investigation for you, which means that you can view detail metrics in the anomaly description. In the following figure, you can see details such as which client and server IP addresses are linked to an unusual number of DNS lookup failures, as well as the host query that could not be resolved. This information helps you immediately begin your investigation into the root cause of this anomaly.



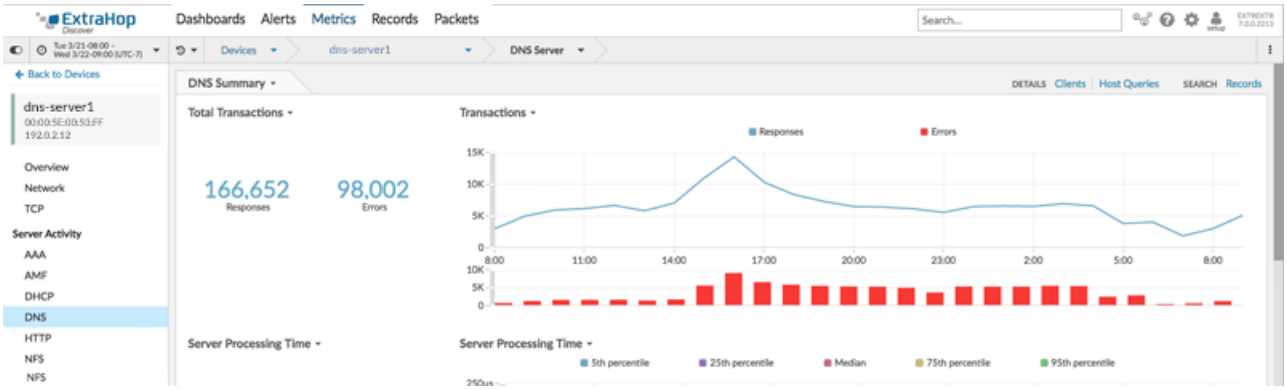
However, if you want to further investigate other metrics related to anomalous network behavior, you can navigate to a protocol page in the Discover or Command appliance.

The following example shows you how to investigate an anomalous DNS lookup failure for a DNS server by navigating to a protocol page, and then find related detail metrics for DNS record types associated with the issue.

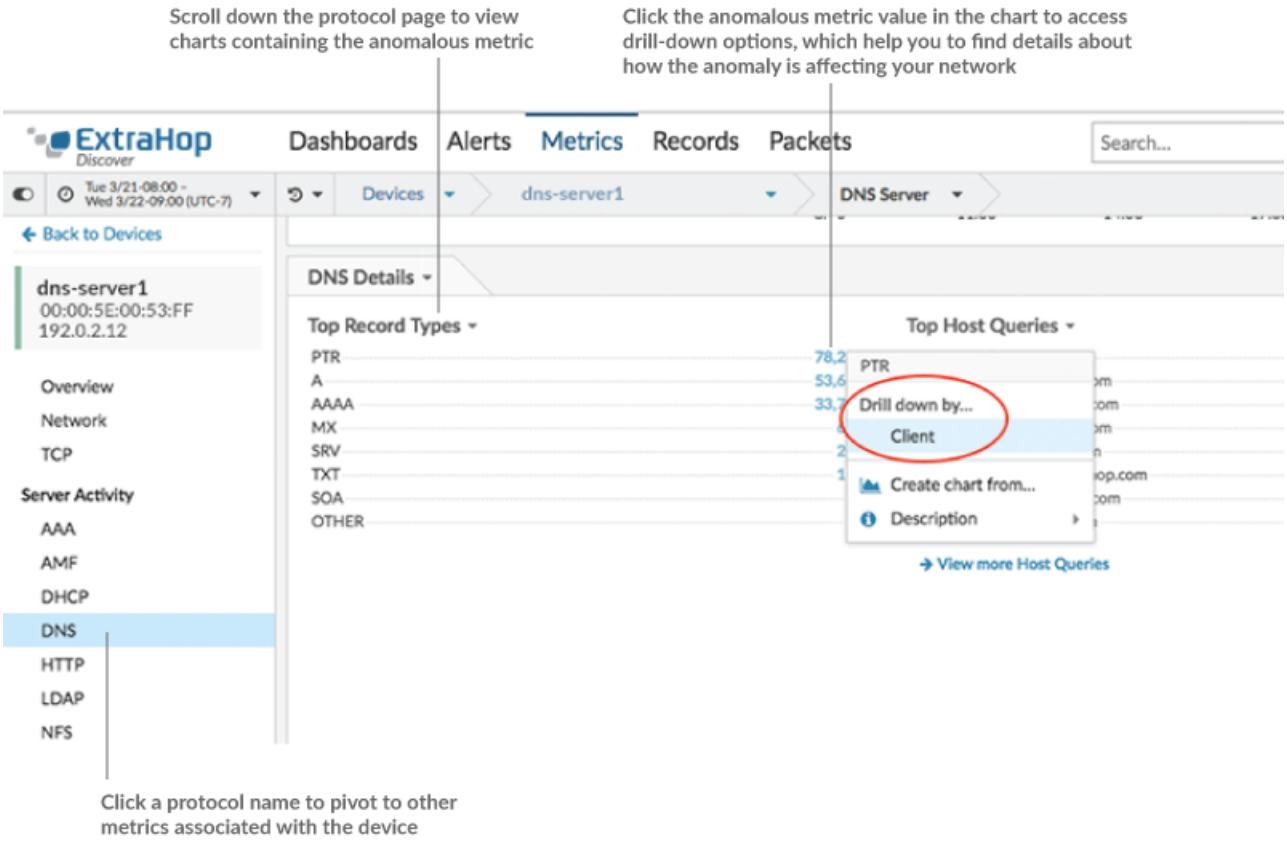
1. Log into the Web UI on the Discover appliance, click **Alerts**, and then click **Anomalies** in the left pane.
2. Find the anomaly that you want to investigate.
3. Click the anomaly title and then select the application or device name from the drop-down, as shown in the figure below.



A protocol page for the device or application appears, which displays all of the metric data associated with that specific device or application, as shown in the figure below.



4. From a protocol page, you can then drill down on metrics to find specific details, and pivot to other protocols to find related metrics, as shown in the figure below.



Tip: To share the anomaly with other ExtraHop users, click the anomaly title and then select **Direct link to anomaly**. An anomaly page with the selected anomaly appears. Copy the URL from the browser window. The URL links directly to the anomaly in the Discover appliance with the same time interval.

Next steps

- Generate an activity map
- Drill down on metrics from device or application protocol pages