Erkunden Sie Metriken im ExtraHop-System, um DNS-Fehler zu untersuchen

Veröffentlicht: 2024-04-10

Das DNS-Protokoll (Domänenname System) ist für die Unterstützung des Internetverkehrs von entscheidender Bedeutung. Es funktioniert oft ohne Probleme. DNS-Server sind in IT-Umgebungen jedoch häufig falsch konfiguriert oder überlastet, was die Internetleistung beeinträchtigen kann.

Es gibt viele Möglichkeiten, DNS-Metriken im ExtraHop-System zu untersuchen. In dieser exemplarischen Vorgehensweise zeigen wir Ihnen, wie Sie DNS-Metriken in einem Dashboard, navigieren Sie zu Seiten mit dem DNS-Protokoll und gehen Sie detailliert auf interessante Messwerte ein, um potenziell betroffene Geräte zu identifizieren.

Insbesondere lernen Sie, wie Sie die folgenden Fragen beantworten können:

- Gibt es ein Netzwerk- oder DNS-Problem, das die Internetleistung beeinträchtigt?
- Wie viele DNS-Fehler gibt es in meinem Netzwerk?
- Welche Clients sind von DNS-Problemen betroffen?

Für die Interpretation von DNS stehen zusätzliche Ressourcen zur Verfügung:

- Erfahren Sie mehr über die Interpretation von DNS-Metriken im ExtraHop-System, indem Sie sich unser Online-Schulungsmodul ansehen. Kurzer Blick: DNS.
- Erfahren Sie mehr über problematische DNS-Abfragen und Fehler, die Sie in Ihrer eigenen Umgebung überwachen können, indem Sie den ExtraHop DNS-Paket. Dieses Paket enthält ein Dashboard mit vorkonfigurierten Diagrammen und detaillierten Erläuterungen zu wichtigen DNS-Fehlern.
- Erfahren Sie, wie ein Dashboard zur Überwachung von DNS-Fehlern erstellen.

Voraussetzungen

- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Referenz zu Protokollmetriken und der FAQ zu Metriken.
- Sie müssen Zugriff auf ein ExtraHop-System mit DNS-Serververkehr haben, oder Sie können diese exemplarische Vorgehensweise in der ExtraHop-Demo.

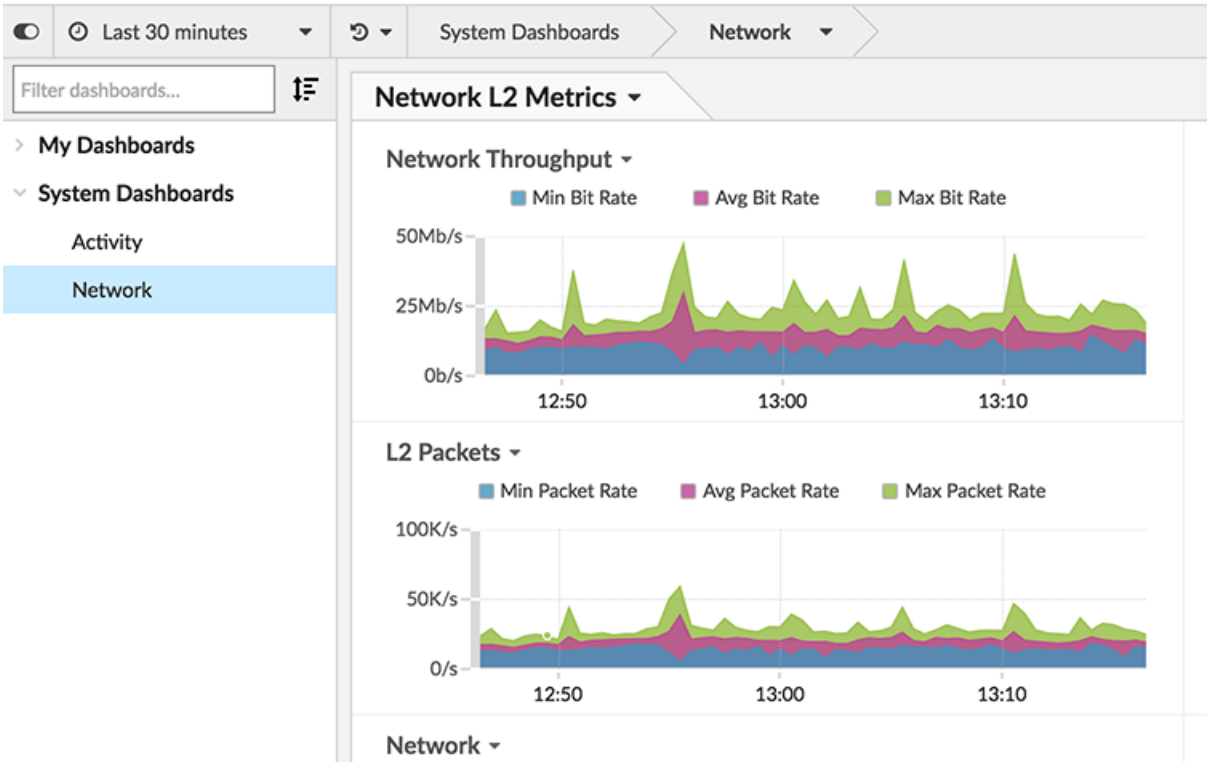
Identifizieren Sie DNS-Probleme mit System-Dashboards

Wenn ein langsames Internetproblem gemeldet wird, schauen Sie in den System-Dashboards nach, ob das Problem mit dem Netzwerkdurchsatz oder dem DNS-Protokoll zusammenhängt.

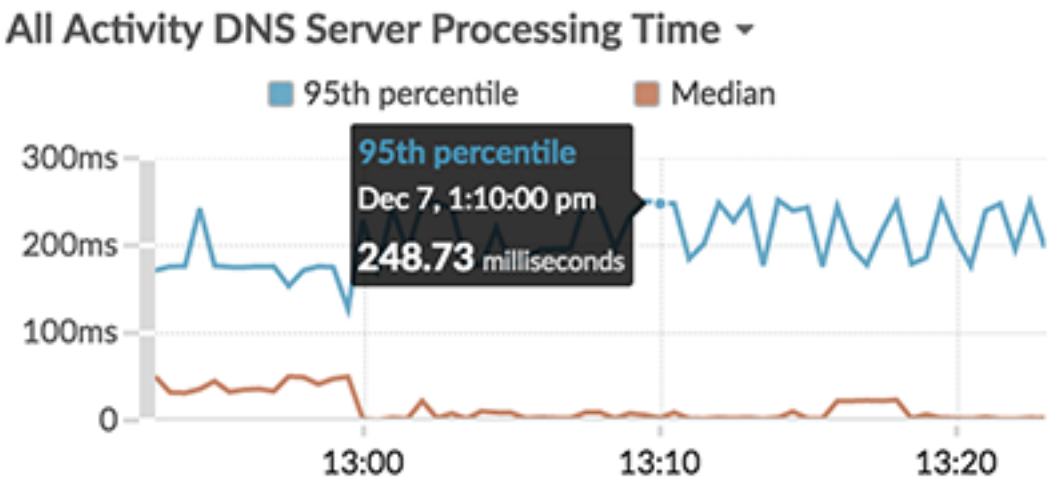
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie in der Navigationsleiste oben links auf die globale Zeitauswahl und wählen Sie **Letzte 7 Tage**, und klicken Sie dann auf **Speichern**.

   Hinweis: Wenn Sie das globale Zeitintervall ändern, haben Sie die Möglichkeit, das Netzwerk- und Protokollverhalten zu sehen, das vor dem erkannten Problem aufgetreten ist.
3. klicken **Armaturenbretter**, und klicken Sie dann auf **Netzwerk** in der System-Dashboards Sammlung.
4. Bestätigen Sie, dass Netzwerkdurchsatz und L2-Pakete Diagramme zeigen normale oder konsistente Spitzen, ähnlich der Abbildung unten. Eine große Diskrepanz zwischen Höchstraten und Durchschnittspreisen kann darauf hindeuten, dass Netzwerkprobleme die Internetleistung beeinträchtigen. Andernfalls setzen Sie Ihre Untersuchung der DNS-Metriken fort.

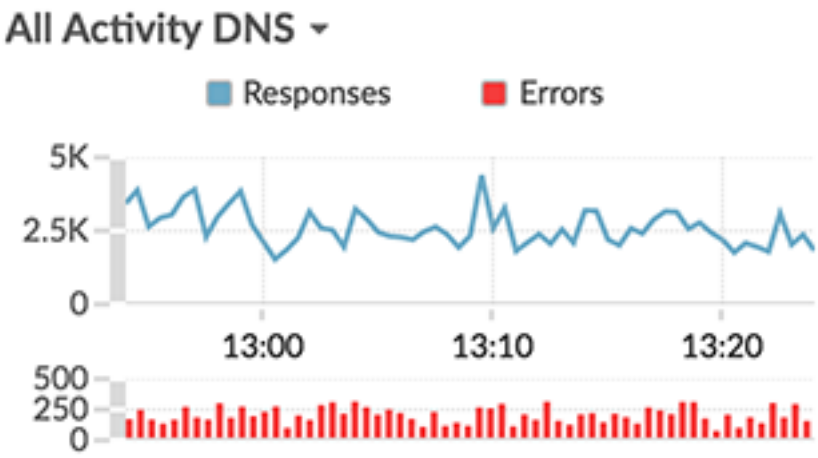
© 2024ExtraHop Networks, Inc. Alle Rechte vorbehalten.



5. klicken **Aktivität** in der System-Dashboards Sammlung.
6. Scrollen Sie nach unten zum Verarbeitungszeit für DNS-Server mit allen Aktivitäten und DNS für alle Aktivitäten Diagramme.
   a) Die Verarbeitungszeit für DNS-Server mit allen Aktivitäten Das Diagramm zeigt Ihnen die Zeit zwischen dem letzten Paket einer DNS-Anfrage von einem Client und dem ersten Paket einer DNS-Antwort vom Server. Bewegen Sie den Mauszeiger über den Median, um die Verarbeitungszeit zum gleichen Zeitpunkt zu vergleichen. Ein großer Unterschied zwischen dem Medianwert und dem 95. Perzentil deutet darauf hin , dass mit einem DNS-Server in Ihrem Netzwerk möglicherweise etwas nicht stimmt.



   b) Die DNS für alle Aktivitäten Das Diagramm korreliert Antworten und Fehler. Ein Anstieg der Fehler kann zu Verzögerungen von zwei bis vier Sekunden für Clients, Server, Anwendungen und Kunden führen. In der Abbildung unten sieht der Anteil der Antworten auf Fehler konsistent aus.



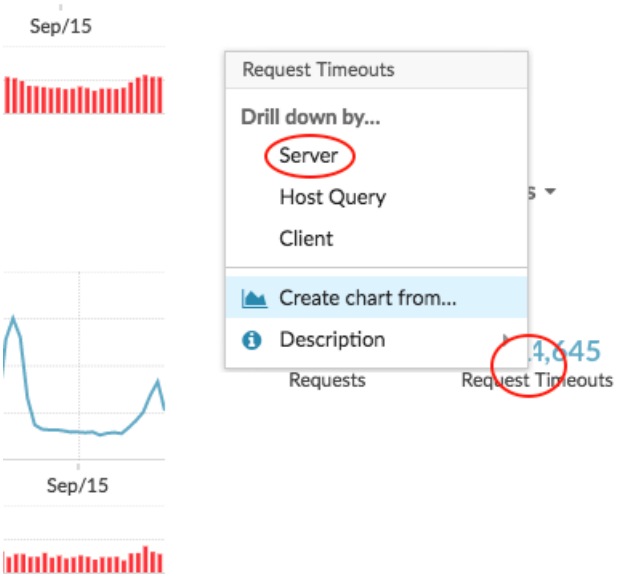
Basierend auf diesen Dashboard-Diagrammen scheint der Netzwerkdurchsatz in Ordnung zu sein, aber die Verarbeitungszeit des DNS-Servers scheint ungewöhnlich zu sein. Als Nächstes sollten wir weitere DNS-Servermetriken untersuchen, um die Ursache für die Verlangsamung zu ermitteln.

Die Anzahl der DNS-Anforderungs-Timeouts anzeigen

Die DNS-Metrik Request Timeouts weist darauf hin, dass eine DNS-Anfrage nicht erfüllt werden konnte. DNS-Server, die Anfragen nicht erfüllen, können sich negativ auf die Anwendung- und Internetleistung auswirken. Sehen wir uns die Gesamtzahl der Anforderungs-Timeouts für DNS-Server in unserem Netzwerk auf einer Protokollseite an. Die Protokollseite für die All Activity-Anwendung bietet einen Überblick über wichtige Messwerte für alle Aktivitäten in Ihrem Netzwerk, einschließlich DNS-Protokollaktivitäten. Wir können dann einen genaueren Blick darauf werfen, bei welchen DNS-Servern ein Timeout auftritt.

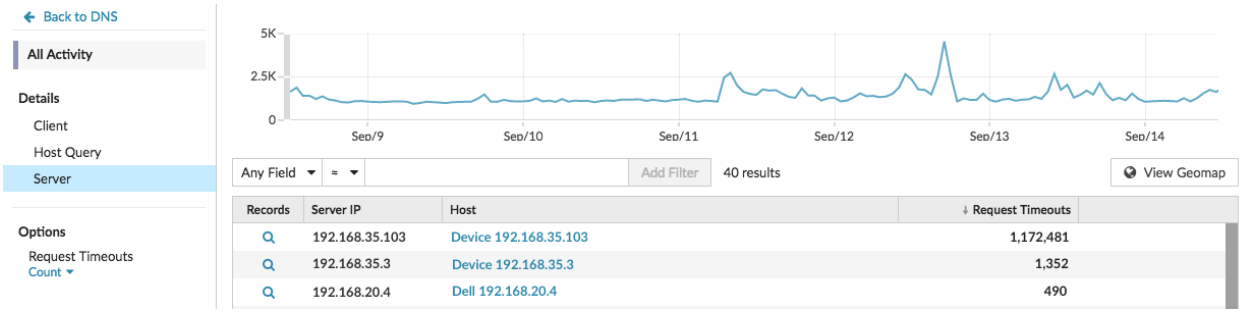
1. Klicken Sie im Aktivitäts-Dashboard auf **DNS für alle Aktivitäten** Titel des Diagramms.
2. In der Gehe zur Anwendung... Abschnitt des Drop-down-Menüs, klicken Sie auf **DNS für alle Aktivitäten**.
   Die Protokollseite All Activity wird angezeigt.
3. Klicken Sie im linken Bereich auf **DNS**.
4. Sehen Sie sich die Anzahl der an Timeouts anfordern. In der Abbildung unten ist die Zahl hoch (1.174.645) und es lohnt sich, weiter untersucht zu werden.

5. Klicken Sie auf den Metrikwert für Request Timeouts und wählen Sie dann **Server**, wie in der Abbildung unten gezeigt.



Es wird eine Seite mit Detail-Metrik angezeigt, auf der alle Server-IP-Adressen in Ihrem Netzwerk mit Anforderungs-Timeouts angezeigt werden.

6. Beachten Sie, welche Geräte die meisten Anforderungs-Timeouts haben. In der Abbildung unten ist dies Gerät 192.168.35.103.

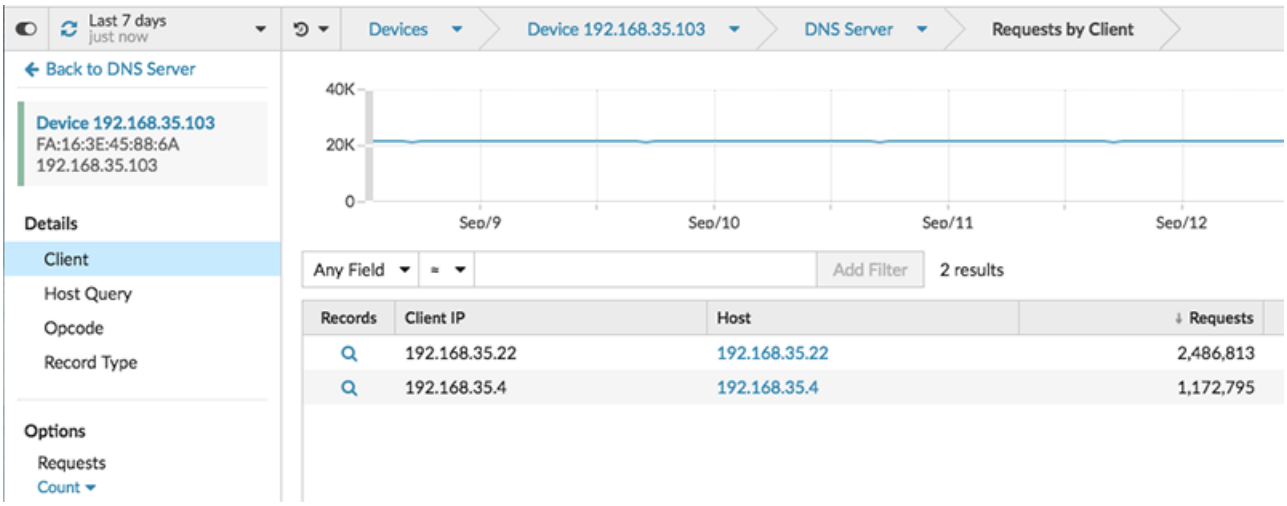


7. In der Gastgeber Klicken Sie in der Spalte auf den Namen des Gerät mit der höchsten Anzahl von Anforderungs-Timeouts.
   Eine neue Protokollseite wird angezeigt, auf der spezifische Metriken für Gerät 192.168.35.103 angezeigt werden. Jetzt können wir untersuchen, welche Clients von diesem DNS-Server betroffen sind.

Finden Sie die Clients, die von DNS-Anforderungs-Timeouts betroffen sind

Sie können jetzt feststellen, welche Clients Anfragen an diesen DNS-Server gesendet haben und welche möglicherweise von DNS-Anforderungs-Timeouts betroffen sind.

1. Klicken Sie auf der Protokollseite für Gerät 192.168.35.103 auf **DNS** in der Serveraktivität Abschnitt im linken Bereich.
2. In der BOHREN Abschnitt oben auf der Seite, klicken Sie **Kunden**.



Es wird eine Seite mit Detail-Metrik angezeigt, auf der alle Client-IP-Adressen angezeigt werden , die Anfragen an den DNS-Server gesendet haben.

Nächste Schritte
Auf dieser Seite mit Detail-Metrik können Sie auch erfahren, welche Host-Abfragen und Datensatztypen in den Anfragen enthalten waren, indem Sie eine Option in der Einzelheiten Abschnitt des linken Bereichs. Oder untersuchen Sie die zugehörigen Kennzahlen für jeden Client, indem Sie auf den Link in der Gastgeber Spalte.

Auf der Grundlage der von Ihnen gesammelten Daten können Sie sich nun an das Team wenden, das für die Wartung dieses speziellen DNS-Servers verantwortlich ist, da dieser möglicherweise falsch konfiguriert ist oder andere Probleme auftreten.