Überwachen Sie DNS-Fehler in einem Dashboard

Veröffentlicht: 2024-01-31

Das Domain Name System (DNS) ist ein unverzichtbarer Dienst für die Auflösung von Hostnamen in IP-Adressen. Jedes System, das andere Systeme lokalisieren und mit ihnen kommunizieren muss, hängt von DNS ab.

DNS ist zwar in der Regel ein robuster Dienst, über den Sie sich vielleicht keine Gedanken machen müssen, aber DNS-Serverfehler können die Endbenutzererfahrung bei E-Mails, Authentifizierungssystemen, Websites und Datenbanken verheerend beeinflussen.

Um zu überwachen, wann und wo DNS-Fehler in Ihrem Netzwerk auftreten, empfehlen wir Ihnen, ein Dashboard im ExtraHop-System zu erstellen. Dashboards enthalten mehrere Arten von Diagrammen, die verschiedene Arten von Informationen zu einer einzelnen Metrik enthalten, was Aufschluss über die zugrunde liegende Ursache von DNS-Fehlern geben kann.

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie ein Dashboard erstellen, um die folgenden Fragen zu beantworten:

- Wie viele DNS-Fehler habe ich?
- Wie hoch ist der Prozentsatz der DNS-Fehler in meinem Netzwerk?
- Wann sind die DNS-Fehler aufgetreten?
- Welche Abfragen verursachen DNS-Fehler?
- Welche DNS-Server geben die Fehler zurück?
- Beeinträchtigen DNS-Fehler die Leistung meiner anderen Server (wie Datenbank oder Anwendungen)?

Voraussetzungen

- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das über eingeschränkte oder vollständige Schreibrechte verfügt.
- Ihr ExtraHop-System muss auch Netzwerkdaten mit DNS-Verkehr haben.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Dashboards Thema.

Wenn Sie keinen Zugriff auf DNS-Serverdaten oder die entsprechenden Rechte haben, können Sie diese exemplarische Vorgehensweise in der ExtraHop-Demo.

Erstellen Sie ein Dashboard

Gehen Sie wie folgt vor, um Ihr eigenes Dashboard zur Anzeige von DNS-Metriken zu erstellen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Armaturenbretter**.
3. Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke und wähle **Neues Dashboard** um ein leeres Dashboard zu erstellen.
4. Geben Sie einen Namen für Ihr Dashboard in der **Titel** Feld. Geben Sie für diese exemplarische Vorgehensweise ein `DNS-Fehler`.
5. klicken **Erstellen**. Wenn Sie ein neues Dashboard erstellen, wird ein Arbeitsbereich in einem bearbeitbaren Layoutmodus geöffnet. Dieser Arbeitsbereich enthält eine einzelne Region und zwei leere Widgets: ein Diagramm und ein Textfeld.

6. Textfeld-Widgets können benutzerdefinierten erklärenden Text zu einem Dashboard oder Diagramm enthalten. Für diese exemplarische Vorgehensweise werden wir jedoch keinen Text hinzufügen. Löschen Sie das Textfeld, indem Sie die folgenden Schritte ausführen:
   a) Klicken Sie auf das Befehlsmenü ⋮ in der oberen rechten Ecke des Textfeld-Widgets und wählen **Löschen**.
   b) klicken **Widget löschen**.

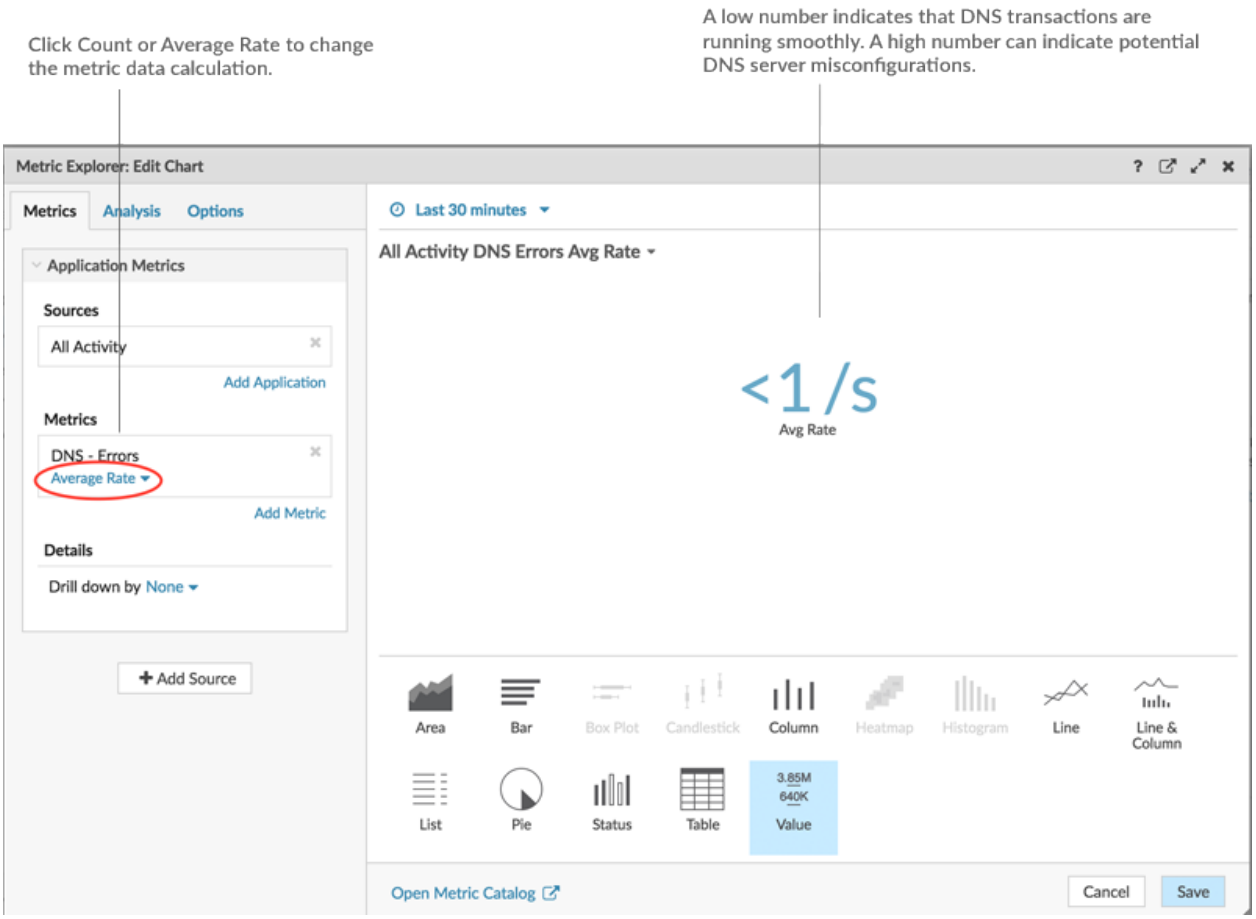
Nächste Schritte
Fügen wir dem leeren Diagramm DNS-Fehlermetriken hinzu.

Wie viele Fehler habe ich?

Diese Schritte zeigen Ihnen, wie Sie ein Diagramm erstellen, um die DNS-Fehlerrate für ein bestimmtes Zeitintervall anzuzeigen.

Um in dieser exemplarischen Vorgehensweise Dashboard-Diagramme zu erstellen, wählen Sie die Anwendung All Activity als Quelle aus. All Activity ist eine Metrikquelle, die standardmäßig für alle Benutzer verfügbar ist und Messwerte zu allen Geräten enthält, die in Ihrem Netzwerk erkannt wurden.

1. Klicken Sie in Ihrem neu erstellten Dashboard auf das leere Diagramm-Widget, um den Metric Explorer zu öffnen.
2. klicken **Quelle hinzufügen**.
3. Geben Sie im Feld Quellen Folgendes ein `Alle Aktivitäten` um die Ergebnisse zu filtern, und wählen Sie dann **Alle Aktivitäten**.
4. Geben Sie im Feld Metriken Folgendes ein `DNS-Fehler` um die Ergebnisse aus allen verfügbaren Metriken zu filtern, und wählen Sie dann **DNS-Fehler**.
5. Klicken Sie unten auf der Seite auf **Wert** Diagramm.
6. klicken **Zählen** und wähle **Durchschnittliche Rate**.



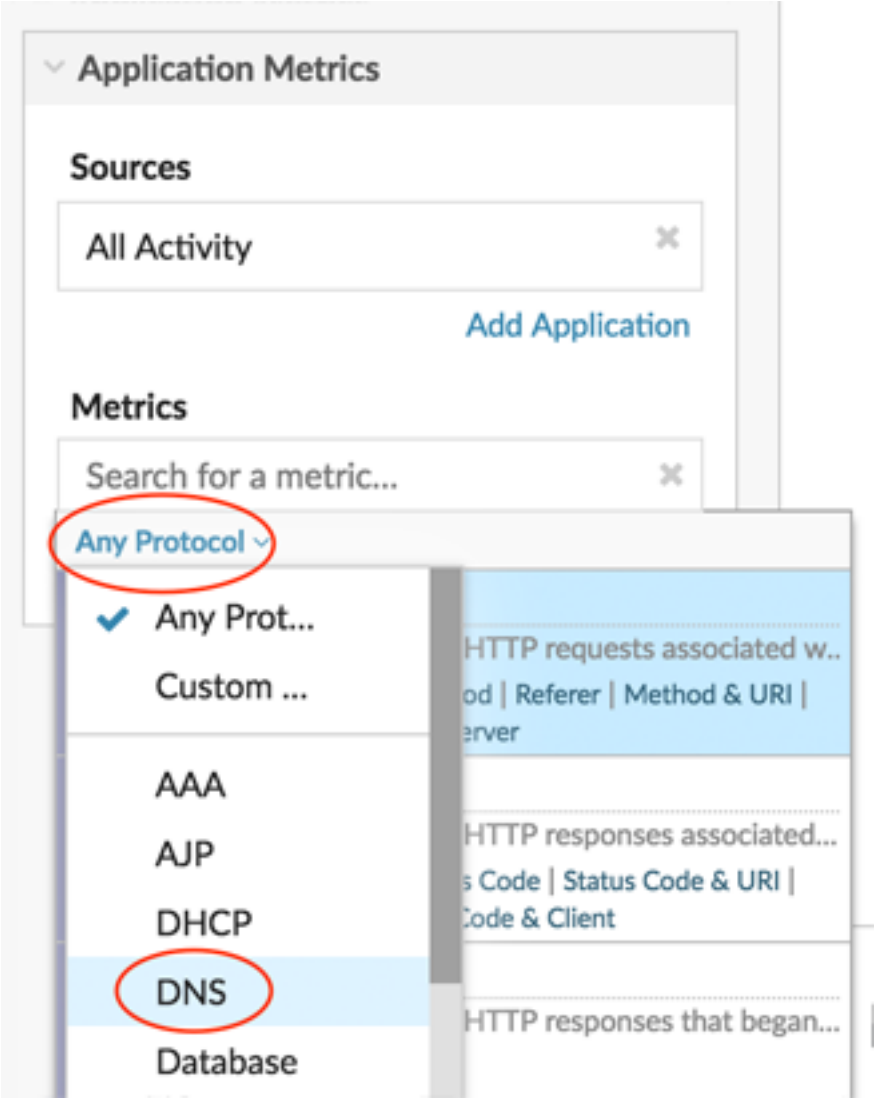
7. klicken **Speichern** um zu Ihrem Dashboard zurückzukehren.

Nächste Schritte
Lassen Sie uns weitere DNS-Fehlerdiagramme hinzufügen, um ein umfassenderes Bild der DNS-Fehler in Ihrem Netzwerk zu erhalten.

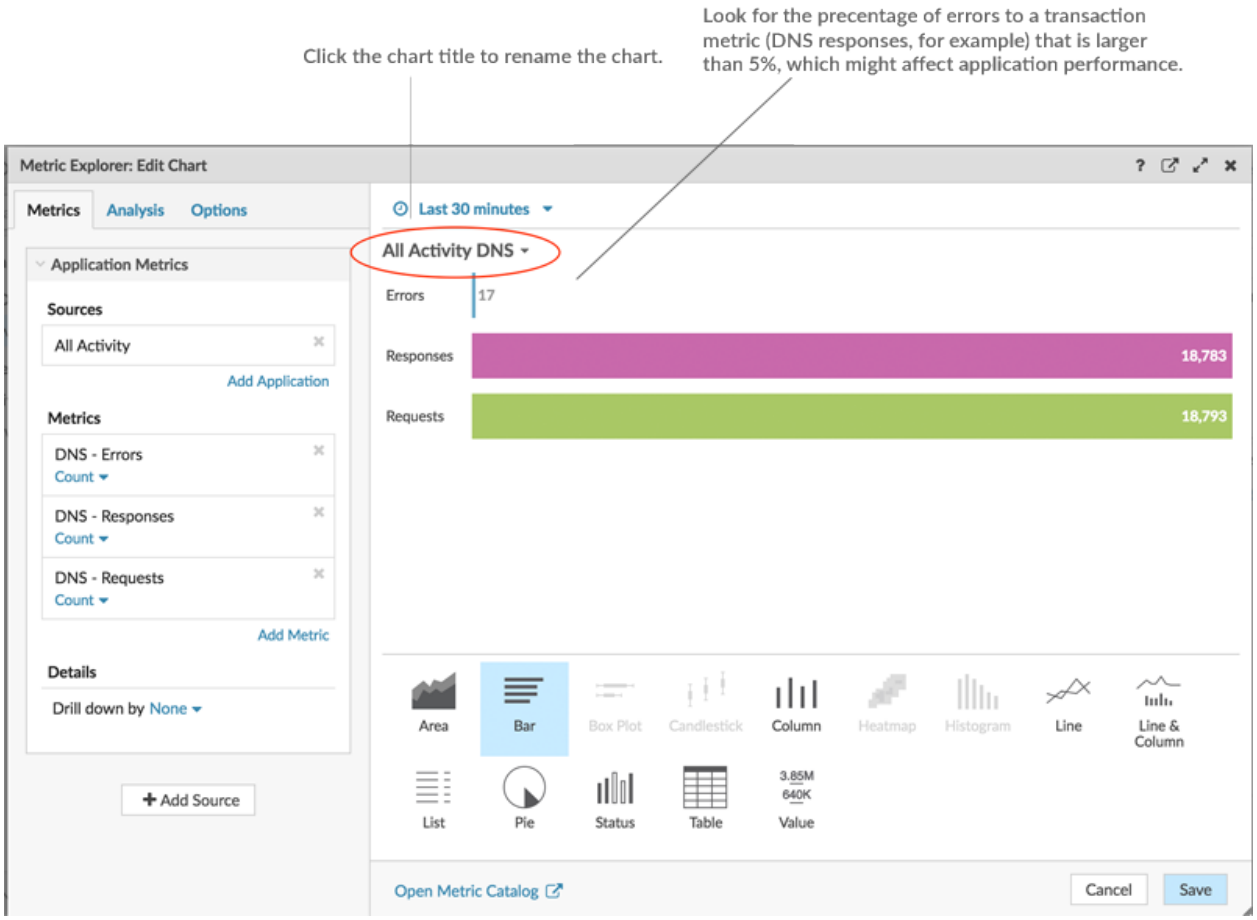
Wie viel Prozent der Fehler treten in meinem Netzwerk auf?

Wenn Sie die Anzahl der DNS-Fehler mit der Anzahl der DNS-Transaktionen (Anfragen und Antworten) vergleichen, können Sie den Umfang der DNS-Probleme in Ihrem Netzwerk einschätzen.

1. Klicken Sie unten auf der Seite auf ein Diagramm-Widget und ziehen Sie es in den leeren Bereich neben dem Diagramm mit der DNS-Fehlerrate.
2. Klicken Sie auf das Diagramm.
3. klicken **Quelle hinzufügen** und wähle **Alle Aktivitäten**.
4. Klicken Sie im Feld Metriken auf **Beliebiges Protokoll** und wähle **DNS**. Mit dieser Tastenkombination können Sie Ihre Suche nach Metriken nach Protokoll eingrenzen.



5. Typ `Fehler` um Ergebnisse zu filtern und dann auszuwählen **DNS-Fehler**.
6. Klicken Sie unten auf der Seite auf **Bar** Diagramm.
7. klicken **Metrik hinzufügen**.
8. klicken **Beliebige Protokolle** und wähle **DNS** aus dem Drop-down-Menü.
9. Typ `Antworten` und wähle **DNS-Antworten**.
10. klicken **Metrik hinzufügen**.
11. klicken **Beliebige Protokolle** und wähle **DNS** aus dem Drop-down-Menü.
12. Typ `Anfragen` und wähle **DNS-Anfragen**.
13. Klicken Sie auf den Diagrammtitel und wählen Sie **Umbenennen**. Typ `Prozentualer Fehleranteil` im Feld für den benutzerdefinierten Titel.



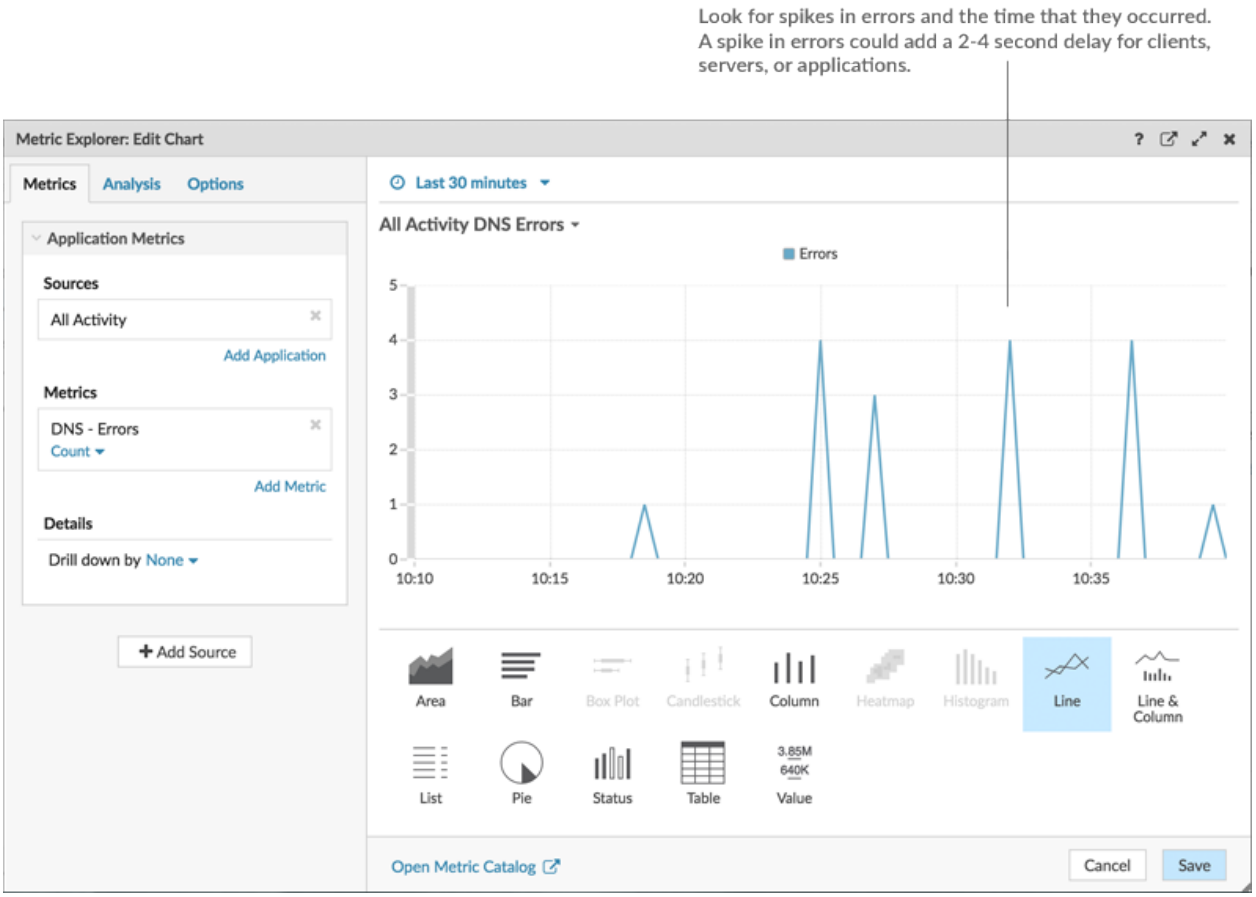
14. klicken **Speichern**.

Nächste Schritte
Sie können jetzt das Verhältnis von DNS-Fehlern zu DNS-Transaktionen berechnen.

Wann sind die DNS-Fehler aufgetreten?

Nachdem Sie den Umfang der DNS-Fehler ermittelt haben, schauen wir uns an, wann die Fehler aufgetreten sind und wie sie sich im Laufe der Zeit verändert haben.

1. Klicken Sie auf ein neues Diagramm-Widget und ziehen Sie es vom unteren Rand der Seite in eine leere Stelle in der Region.
2. Klicken Sie auf das Diagramm.
3. klicken **Quelle hinzufügen**, wählen **Alle Aktivitäten**, und wählen Sie dann **DNS-Fehler**.
4. Klicken Sie unten auf der Seite auf **Linie** Diagramm.



5. klicken **Speichern**.

Nächste Schritte
Sie haben jetzt drei Diagramme, mit denen Sie den Zustand der DNS-Transaktionen in Ihrem Netzwerk visualisieren können. Als Nächstes fügen wir Diagramme hinzu, die Ihnen helfen, die Ursache von DNS-Fehlern genauer zu untersuchen und zu sehen, welche Auswirkungen sie auf Ihr gesamtes Netzwerk haben.

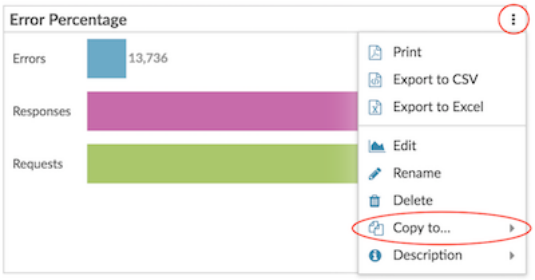
Welche Host-Abfragen verursachen die DNS-Fehler?

Eine Hostabfrage wird von einem Client gesendet, um die IP-Adresse für einen Hostnamen (z. B. für „extrahop.com“) von einem DNS-Server abzurufen. Wenn der DNS-Server auf die Anfrage mit einem Fehler antwortet, ist der Server möglicherweise für die mit dem Hostnamen verknüpfte Domäne falsch konfiguriert.

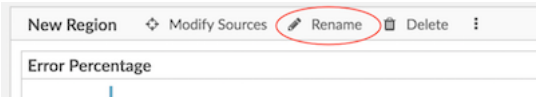
Sie können die DNS-Fehlermetrik in einem Diagramm aufschlüsseln, um bis zu 20 der häufigsten Hostnamenabfragen anzuzeigen, die zur Gesamtzahl der DNS-Fehler in Ihrem Netzwerk beigetragen haben.

Bevor Sie Ihrem Dashboard ein neues Host-Query-Diagramm hinzufügen, fügen wir dem Dashboard zunächst eine weitere Region hinzu, um die aktuellen Diagramme besser in logische Gruppen zu organisieren.

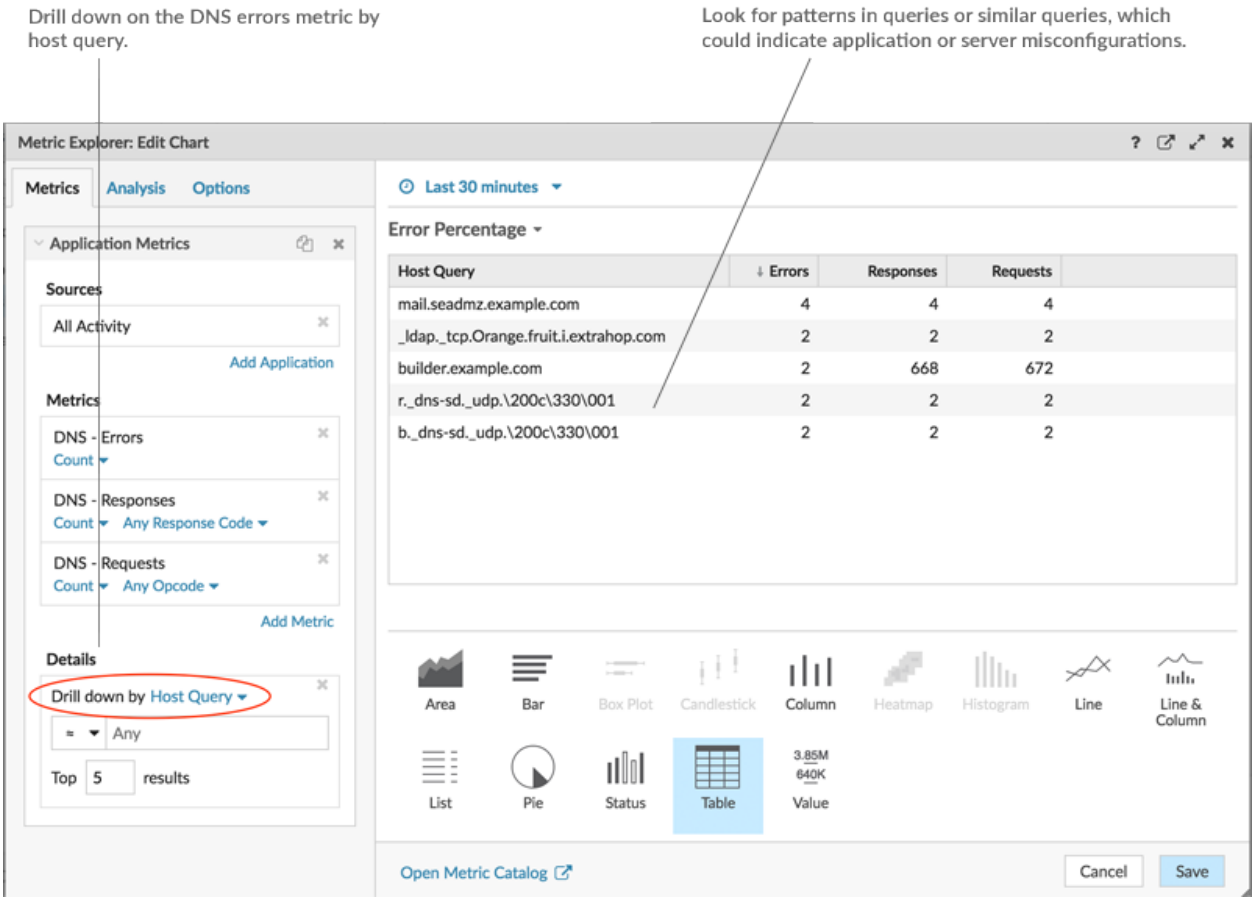
1. Klicken Sie in der Tabelle „Fehlerprozentsatz“ auf das Befehlsmenü ⋮ in der oberen rechten Ecke.



2. Bewegen Sie den Mauszeiger darüber **Kopieren nach...** und wählen Sie den Namen Ihres Dashboard aus dem Menü aus. In diesem Schritt wird eine Kopie des Diagramms in einer neuen Region erstellt. Die zuletzt erstellten Dashboards sind unten im Menü aufgeführt.
3. Klicken Sie in der neuen Region auf **Umbenennen**. Typ `Details zum DNS-Fehler` und klicken **Speichern**.



4. Klicken Sie auf das Diagramm.
5. Klicken Sie auf den Diagrammtitel und geben Sie **DNS-Fehler nach Host-Abfrage**.
6. Klicken Sie unten auf der Seite auf **Tabelle**.
7. Klicken Sie im Abschnitt Details auf **Drilldown nach <None>** und wähle **Host-Abfrage**.



Hinweis: Um mehr Abfragen anzuzeigen, geben Sie eine größere Zahl in das Feld Top-Ergebnisse ein. Sie können bis zu 20 Drilldown-Elemente in einem Dashboard-Diagramm anzeigen.

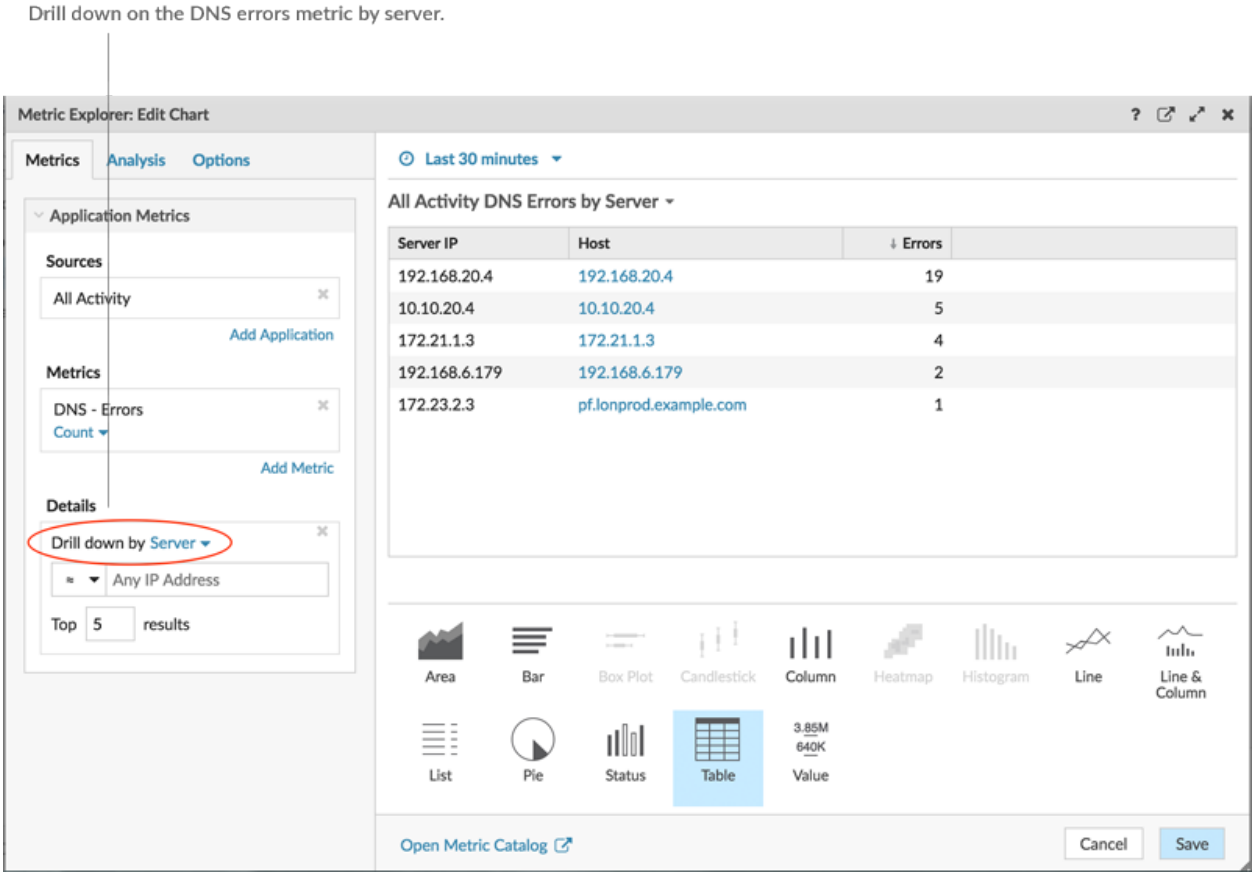
8. klicken **Speichern**.

Nächste Schritte
Nachdem Sie Abfragen identifiziert haben, die Fehler nicht lösen oder verursachen, können Sie mit der Problembehandlung der DNS-Serverkonfigurationen in Ihrer Netzwerkumgebung beginnen .

Welche DNS-Server geben Fehler zurück?

Wenn Sie wissen, welche Server DNS-Fehler zurückgeben und wie viele Fehler jeder Server gesendet hat, können Sie DNS-Probleme beheben.

1. Klicken und ziehen Sie die Ecke des Region, um Platz für zwei weitere Diagramme zu schaffen.
2. Klicken Sie auf ein Diagramm-Widget und ziehen Sie es vom unteren Rand der Seite.
3. Klicken Sie auf das Diagramm.
4. Klicken Sie auf Quelle hinzufügen, wählen Sie Alle Aktivitäten und dann DNS-Fehler aus.
5. Klicken Sie unten auf der Seite auf **Tabelle**.
6. Klicken Sie im Abschnitt Details auf **Drilldown nach <None>** und wähle **Server**.



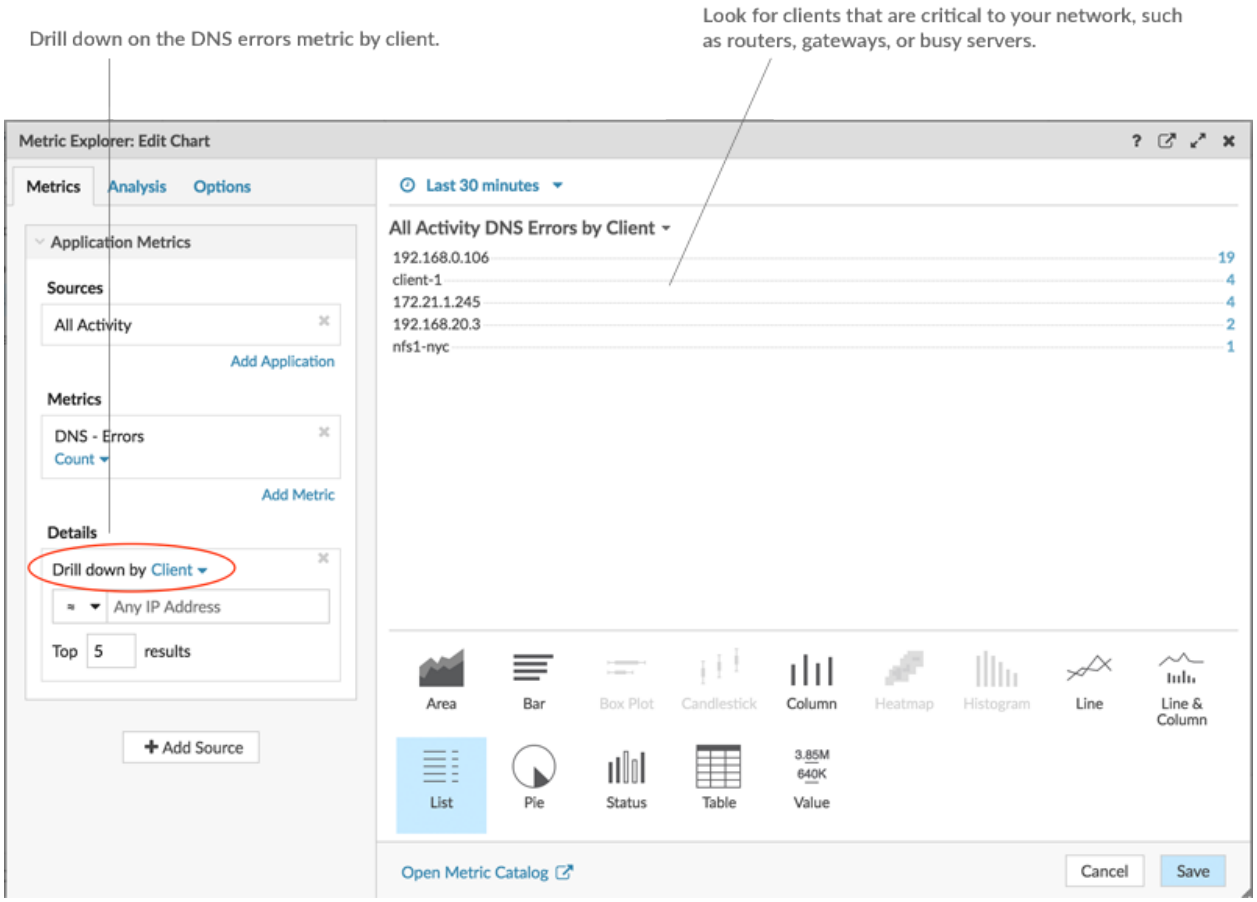
7. klicken **Speichern**.

Nächste Schritte
Sie können jetzt feststellen, welche Server die meisten DNS-Fehler gesendet haben, möglicherweise aufgrund von Serverfehlkonfigurationen.

Beeinträchtigen DNS-Fehler die Leistung meiner anderen Server?

Sie können feststellen, welche Anwendungen, Datenbanken und anderen Server durch DNS-Fehler negativ beeinflusst werden. Lassen Sie uns ein Diagramm erstellen, das die Anzahl der DNS-Fehler nach den Clients aufschlüsselt, die die meisten Fehler erhalten haben.

1. Ziehen Sie ein Diagramm-Widget vom unteren Seitenrand in einen leeren Bereich.
2. Klicken Sie auf das Diagramm.
3. klicken **Quelle hinzufügen**, wählen **Alle Aktivitäten**, und wählen Sie dann **DNS-Fehler**.
4. Klicken Sie unten auf der Seite auf **Liste** Diagramm.
5. Klicken Sie im Abschnitt Details auf **Drilldown nach <None>** und wähle **Kunde**.



Hinweis Sie können Ihrem Listendiagramm eine Sparkline hinzufügen, um zu sehen, wie sich die Anzahl der Metriken für jeden Client im Laufe der Zeit verändert hat. Klicken Sie auf die Registerkarte Optionen und wählen Sie **Sparkline einbeziehen**.

6. klicken **Speichern**.
7. Klicken Sie in der oberen rechten Ecke der Dashboard-Seite auf **Layoutmodus verlassen**.

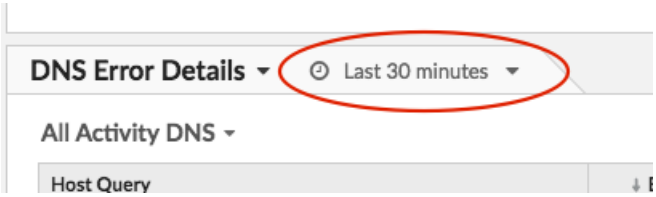
Nächste Schritte

Ihr Dashboard ist fertig! Sie können jetzt DNS-Fehler zur Fehlerbehebung überwachen. In den folgenden Abschnitten finden Sie zusätzliche Tipps zur Analyse von DNS-Problemen in Ihrem Dashboard.

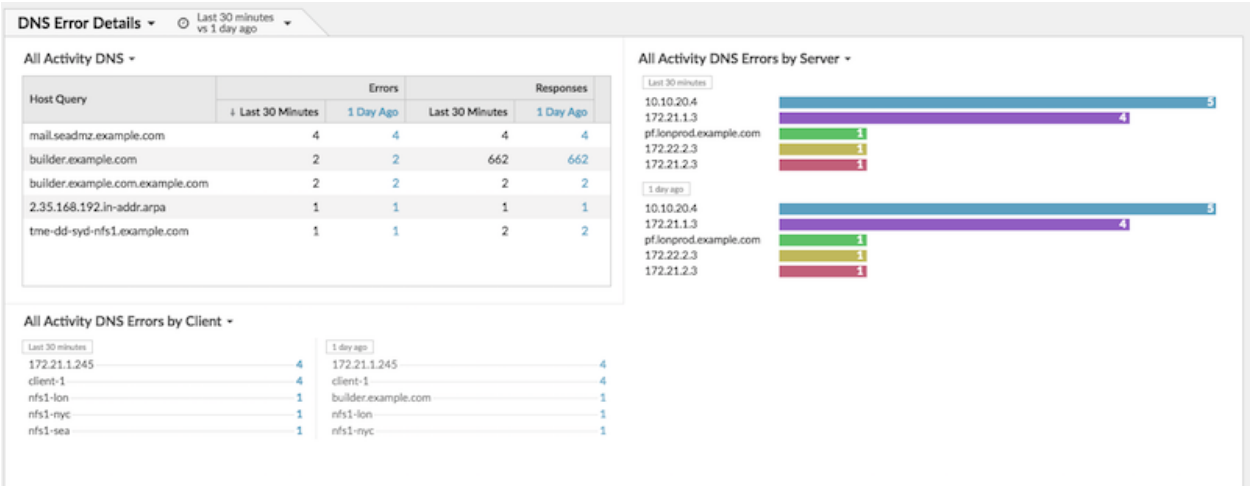
Verschiedene Zeitintervalle vergleichen

Wenn Sie einen Delta-Vergleich von Zeitintervallen auf Ihre Diagramme anwenden, können Sie Änderungen an Daten aus zwei Zeitintervallen nebeneinander sehen.

1. Klicken Sie auf den Titel der Region, „DNS-Fehlerdetails“, und wählen Sie **Region Zeitselektor verwenden**.
2. Klicken Sie neben dem Region-Header DNS-Fehlerdetails auf **Letzte 30 Minuten**.



3. Klicken Sie am unteren Rand des Zeitintervallfensters auf **Vergleiche**. Sie können jetzt zwei Intervalle auswählen, um einen Delta-Vergleich der Metriken aus jedem Zeitraum durchzuführen. Lassen Sie uns für dieses Beispiel die Metriken von gestern mit den letzten 30 Minuten vergleichen.
4. klicken **Speichern**. Sie sehen nun einen Vergleich der Kennzahlen in allen Diagrammen innerhalb der Region, wie in der Abbildung unten dargestellt.



Hinweis Sie können einen Delta-Vergleich für das gesamte Dashboard durchführen, indem Sie das globale Zeitintervall ändern. Das globale Zeitintervall befindet sich in der oberen linken Ecke der Dashboard-Seite.

5. Um den Delta-Vergleich zu entfernen, klicken Sie auf **Letzte 30 Minuten gegenüber vor einem Tag** klicken Sie in der Kopfzeile der Region auf **Delta entfernen**, und klicken Sie dann auf **Speichern**.

Zusätzliche zu überwachende DNS-Metriken

DNS-Fehler sind eine Informationsquelle über den Zustand des DNS-Verkehrs in Ihrem Netzwerk. Die folgende Tabelle enthält zusätzliche Kennzahlen, die Sie zu Ihrem Dashboard hinzufügen können, um die folgenden Fragen zu beantworten:

Frage	DNS-Metrik	Beschreibung
Verwerfen DNS-Server Anfragen?	Timeouts für DNS-Anfragen	DNS-Anfragen, die keine Antwort von einem DNS-Server erhalten, sind potenzielle Engpässe. Server-Timeouts können zu Verlangsamungen und

Frage	DNS-Metrik	Beschreibung
		Ausfällen von Servern, Clients und Anwendungen führen.
Gibt es Sicherheitslücken im Zusammenhang mit DNS?	DNS-Anfragen können Sie nach Hostabfragen aufschlüsseln und nach „WPAD“ oder „ISATAP“ filtern.	Automatische Erkennung von Webproxys (WPAD) und Standortinternes automatisches Tunneladressierungsprotokoll (ISATAP) sind Beispiele für Host-Abfragen, die sich auf bekannte Sicherheitsrisiken beziehen.
Beeinflusst das Netzwerk DNS-Transaktionen?	DNS-Roundtrip-Zeit	Die Round Trip Time (RTT) wird berechnet, indem die Zeit beobachtet wird, die Pakete benötigen, um das Netzwerk zwischen Geräten zu durchqueren. Eine hohe RTT kann auf eine Netzwerklatenz hinweisen.