Drilldown

Veröffentlicht: 2024-11-02

Eine interessante Metrik führt natürlich zu Fragen zu den Faktoren, die mit diesem Metrikwert verbunden sind. Wenn Sie beispielsweise in Ihrem Netzwerk eine große Anzahl von DNS-Anforderungs-Timeouts feststellen, fragen Sie sich möglicherweise, bei welchen DNS-Clients diese Timeouts auftreten. Im ExtraHop-System können Sie ganz einfach einen Drilldown von einer Top-Level-Metrik aus durchführen, um die Geräte, Methoden oder Ressourcen anzuzeigen, die mit dieser Metrik verknüpft sind.

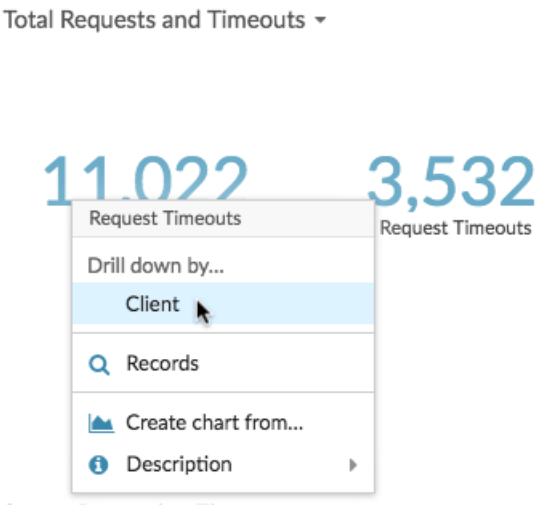
Wenn Sie eine Metrik anhand eines Schlüssels (z. B. einer Client-IP-Adresse, Methode, URI oder Ressource) aufschlüsseln, berechnet das ExtraHop-System eine Topnset von bis zu 1.000 Schlüssel-Wert-Paaren. Anschließend können Sie diese Schlüssel-Wert-Paare untersuchen, die als Metriken detailliert, um zu erfahren, welche Faktoren mit der interessanten Aktivität zusammenhängen.

Drilldown von einem Dashboard oder einer Protokollseite aus

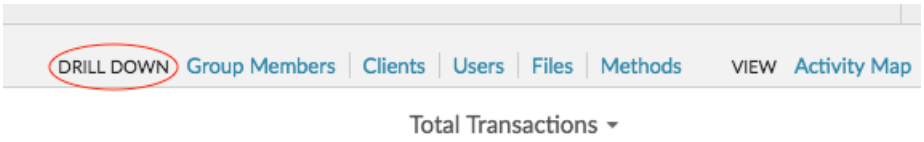
Wenn Sie in einem Diagramm oder einer Legende auf eine Metrik klicken, können Sie sehen, welcher Schlüssel, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Ressource, zu diesem Wert beigetragen hat.

In den folgenden Schritten erfahren Sie, wie Sie eine Metrik finden und anschließend eine Aufgliederung vornehmen können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Finden Sie eine interessante Metrik, indem Sie einen der folgenden Schritte ausführen:
   - klicken **Armaturenbrett**, und wählen Sie dann im linken Bereich ein Dashboard aus. Ein Dashboard mit Metriken wird angezeigt.
   - klicken **Vermögenswerte**, klicken **Gerät**, **Gerätegruppe**, oder **Bewerbung** im linken Bereich. Wählen Sie dann ein Gerät, eine Gruppe oder eine Anwendung aus. Eine Protokollseite mit Metriken wird angezeigt.
   - klicken **Vermögenswerte**, klicken **Netzwerke** im linken Bereich, und wählen Sie dann ein Flow-Netzwerk aus. Eine Protokollseite mit Metriken wird angezeigt.
3. Klicken Sie in der Diagrammlegende auf einen Metrikwert oder eine Metrikbezeichnung, wie in der folgenden Abbildung dargestellt. Es erscheint ein Menü.



Hinweis: Auf einer Protokollseite können Sie auch auf eine Drilldown-Schaltfläche in der Drilldown Abschnitt, der sich in der oberen rechten Ecke der Seite befindet. Die Art der Tastenkombinationen variiert je nach Protokoll.



4. In der Drilldown nach... Abschnitt, wählen Sie einen Schlüssel aus. Eine Seite mit detaillierten Metriken mit Topnset Es wird eine Liste der Metrikwerte nach Schlüssel angezeigt. Auf dieser Seite können Sie bis zu 1.000 Schlüssel-Werte-Paare anzeigen.

Hinweis: Falls verfügbar, klicken Sie auf **Mehr ansehen** Link am unteren Rand eines Diagramms, um die im Diagramm angezeigte Metrik genauer zu untersuchen.

Nächste Schritte

- Untersuchen Sie detaillierte Metriken

Detaillierter Überblick über Netzwerkerfassung und VLAN-Metriken

Klicken Sie auf eine interessante Top-Level-Metrik zur Netzwerkaktivität auf einem Netzwerk einfangen oder VLAN Seite, um zu ermitteln, welche Geräte mit dieser Aktivität verknüpft sind.

Hinweis: Informationen dazu, wie Sie Metriken von einer Seite mit einem Flussnetz oder einer Flow-Netzwerkschnittstelle aus aufschlüsseln können, finden Sie in Drilldown von einem Dashboard oder einer Protokollseite aus Abschnitt.

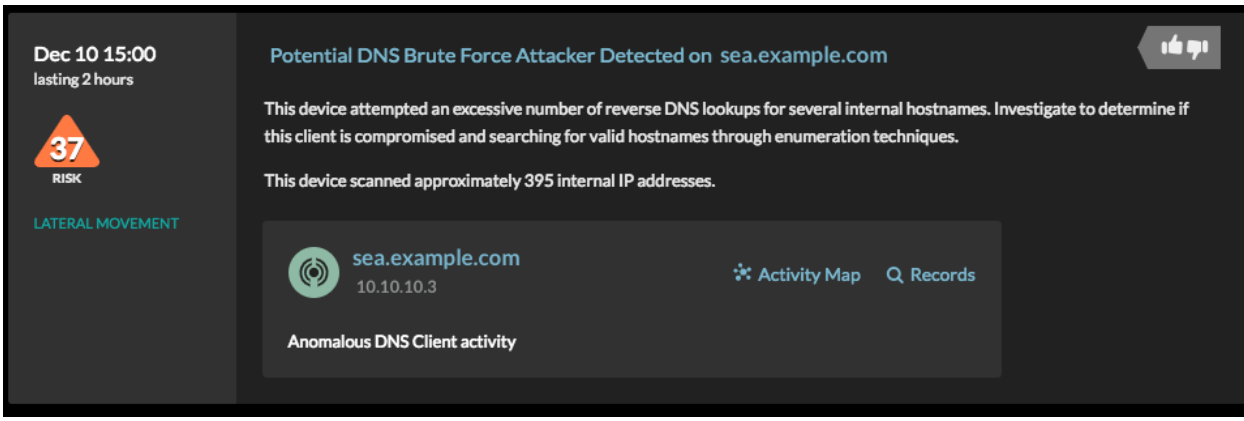
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**.
3. klicken **Netzwerke** im linken Bereich.
4. Klicken Sie auf einen Netzwerk-Capture- oder VLAN-Schnittstellennamen.
5. Klicken Sie im linken Bereich auf einen Netzwerk-Layer, z. B. **L3** oder **L7-Protokolle**. Es werden Diagramme angezeigt, die Metrikwerte für das ausgewählte Zeitintervall anzeigen. Für die meisten Protokolle und Metriken ist ein Gerät Die Tabelle wird auch unten auf der Seite angezeigt.
6. Klicken Sie auf die Diagrammdaten, wodurch die Liste aktualisiert wird, sodass nur die Geräte angezeigt werden, die mit den Daten verknüpft sind.
7. Klicken Sie auf einen Gerätenamen. EIN Gerät Eine Seite wird angezeigt, auf der der Datenverkehr und die Protokollaktivitäten im Zusammenhang mit dem ausgewählten Gerät angezeigt werden.

Drilldown von einer Erkennung aus

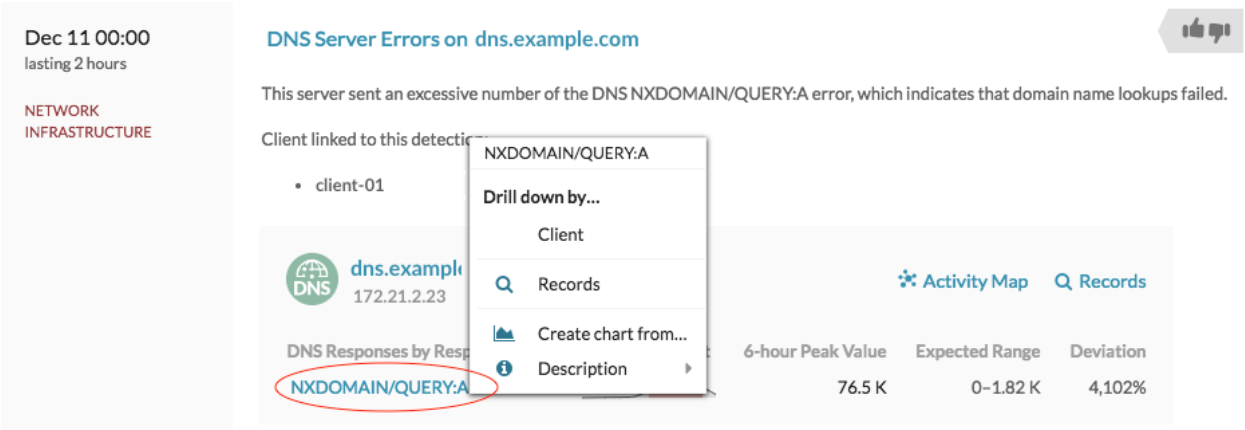
Bei bestimmten Erkennungen können Sie weitere Details zu der Metrik oder dem Schlüssel aufrufen , der zu dem ungewöhnlichen Verhalten beigetragen hat. Der Metrikname oder der Schlüssel wird als Link am Ende einer einzelnen Erkennung angezeigt.

Hinweis: Erkennungen mit Metriken oder Schlüsseln, die keine detaillierten Metriken enthalten, beinhalten keine Drilldown-Option. Erkennungen, die statt einer Metrik nur anomale Protokollaktivitäten anzeigen, beinhalten auch keine Metrik-Drilldown-Option. Sie können z. B. keinen Drilldown zu einer Erkennung von anomalen DNS-Client-Aktivitäten durchführen, wie in der Abbildung unten dargestellt. Klicken Sie stattdessen auf die Links für den Gerät-

oder Anwendungsnamen. **Karte der Aktivitäten**, oder **Rekorde** um mehr über die anomale Aktivität zu erfahren.



1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Erkennungen** oben auf der Seite.
3. Suchen Sie nach einer interessanten Erkennung, die mit einer Metrik verknüpft ist, und klicken Sie auf den Namen oder Schlüssel der Metrik. In der folgenden Abbildung können wir durch Klicken auf den Antwortcode eine Aufschlüsselung aller Clients aufrufen, die DNS-Antworten mit NXDOMAIN/QUERY:A erhalten haben.



4. In der Drilldown nach... Abschnitt, klicken Sie auf eine Taste wie **Kunde**.
   Es wird eine Seite mit Detail-Metrik angezeigt, auf der Sie nach Schlüsseln aufgelistete Metriken untersuchen.

Drilldown von einer Alarm aus

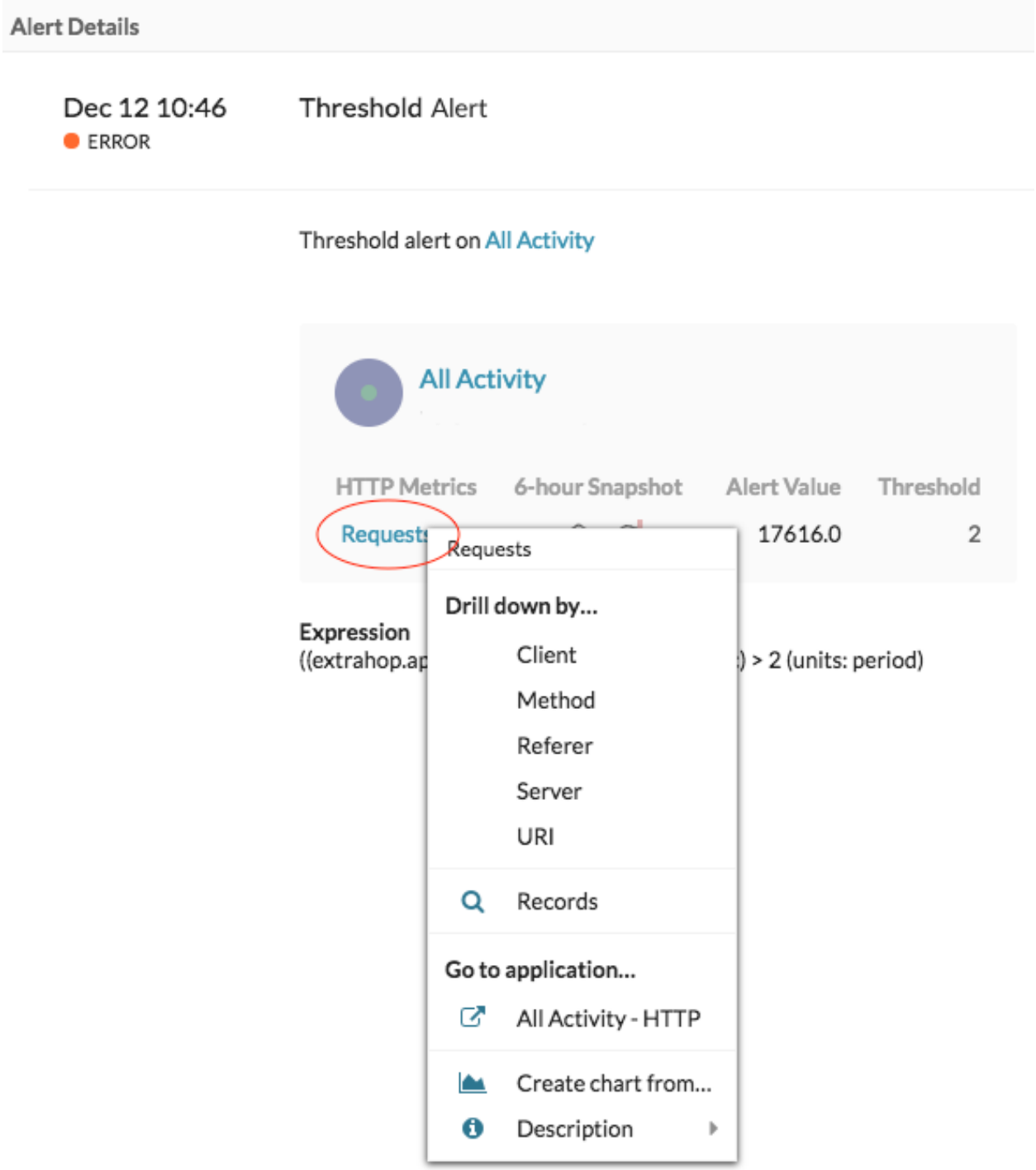
Klicken Sie in einer Schwellenwertwarnung auf den Metriknamen oder Schlüssel, um zu sehen, welcher Schlüssel, z. B. Client, Server, Methode oder Ressource, zu dem Metrikwert oder dem ungewöhnlichen Verhalten beigetragen hat.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Alerts** oben auf der Seite.

Hinweis Sie können auf Benachrichtigungen auch über ein Alert-Widget in einem Dashboard oder unten auf den folgenden Protokollseiten zugreifen:

- Seite „Anwendungsübersicht“
- Seite „Gerätegruppen-Übersicht“
- Seite „Netzwerkübersicht“

3. Klicken Sie auf den Namen einer Schwellenwarnung.
Warndetails werden angezeigt.
4. Klicken Sie auf einen Metriknamen oder -schlüssel, wie in der folgenden Abbildung dargestellt.



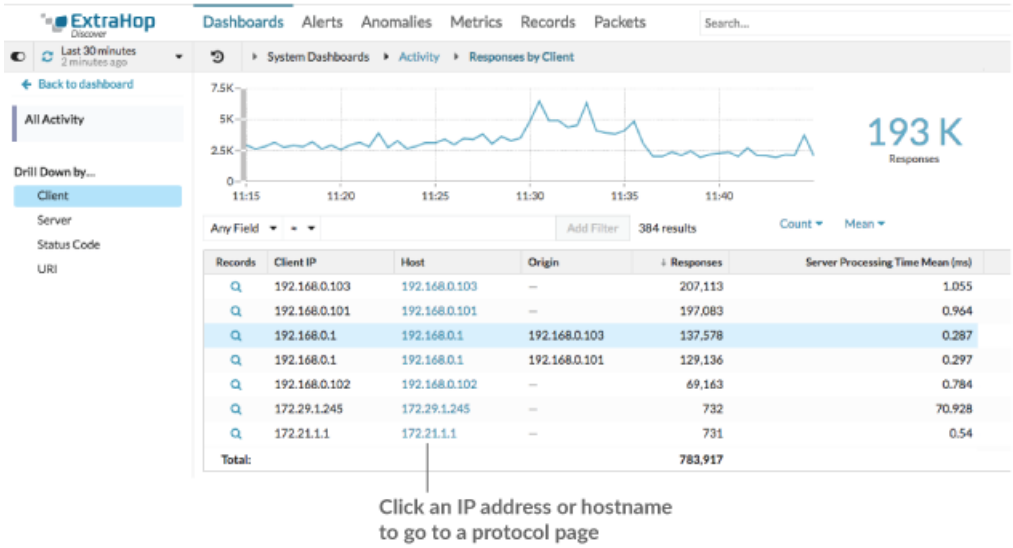
5. In der Drilldown nach Abschnitt, klicken Sie auf eine Taste, z. B. **Kunde**, **Methode**, **Verweiser**, **Server**, oder **URI**.
   Es wird eine Seite mit Detail-Metrik angezeigt, auf der Sie nach Schlüsseln aufgelistete Metriken untersuchen.

Untersuchen Sie detaillierte Metriken

Nachdem Sie eine Metrik von einem Dashboard, einer Protokollseite, einer Erkennung oder einer Alarm aus detailliert untersucht haben, können Sie die Metrikwerte anhand von Schlüsseln auf einer Seite mit den Detail-Metrik untersuchen. Filtern Sie Metrikdaten oder wählen Sie verschiedene Schlüssel wie Statuscodes oder URIs aus, um Daten aus verschiedenen Perspektiven anzuzeigen.

Die folgende Abbildung zeigt, wie Sie Daten auf einer Seite mit Detail-Metrik Metriken filtern, pivotieren, sortieren oder exportieren.

Wenn Sie eine Metrik nach IP, Client oder Server aufgeschlüsselt haben, werden IP-Adressen und Hostnamen (sofern sie anhand des DNS-Datenverkehrs beobachtet wurden) in der Tabelle angezeigt. Zusätzliche Optionen stehen Ihnen jetzt zur Verfügung. Sie können beispielsweise direkt zu einer Client- oder Serverprotokollseite navigieren, wie in der folgenden Abbildung dargestellt.



Ergebnisse filtern

Eine Detailseite kann bis zu 1.000 Schlüssel-Wert-Paare enthalten. Es gibt zwei Möglichkeiten, bestimmte Ergebnisse aus Daten zu finden: Filterergebnisse oder klicken Sie auf eine Taste in der Tabelle, um einen weiteren Drilldown-Filter zu erstellen.

Um die Ergebnisse zu filtern, klicken Sie auf **Beliebiges Feld**, und wählen Sie dann ein Feld aus, das je nach Schlüssel variiert. Zum Beispiel können Sie wählen **Netzwerk-Lokalität** für Client- oder Serverschlüssel. Wählen Sie dann einen der folgenden Operatoren aus:

- Wählen Sie **=** um eine exakte Zeichenkettenübereinstimmung durchzuführen.
- Wählen Sie **≈** um eine ungefähre Zeichenkettenübereinstimmung durchzuführen. Der Operator ≈ unterstützt reguläre Ausdrücke.

  Hinweis: Um ein Ergebnis auszuschließen, geben Sie einen regulären Ausdruck ein. Weitere Informationen finden Sie unter Filter für reguläre Ausdrücke erstellen.
- Wählen Sie **#** um eine ungefähre Zeichenkettenübereinstimmung aus Ihren Ergebnissen auszuschließen.
- Wählen Sie **>** oder **≥** um eine Übereinstimmung mit Werten durchzuführen, die größer als (oder gleich) einem angegebenen Wert sind.
- Wählen Sie **<** oder **≤** um eine Übereinstimmung mit Werten durchzuführen, die kleiner als (oder gleich) einem bestimmten Wert sind.
- Klicken Sie **Filter hinzufügen** um die Filtereinstellungen zu speichern. Sie können mehrere Filter für eine Abfrage speichern. Gespeicherte Filter werden gelöscht, wenn Sie im Bereich Details im linken Bereich einen anderen Schlüssel auswählen.

Um den Filter abzuschließen, geben Sie einen Wert ein, nach dem Sie die Ergebnisse filtern möchten, oder wählen Sie einen Wert aus, und klicken Sie dann auf **Filter hinzufügen**.

Untersuchen Sie Bedrohungsdaten (Nur ExtraHop RevealX Premium und Ultra)

Klicken Sie auf das rote Kamerasymbol zum Ansehen Bedrohungsinformationen Details zu einem verdächtigen Host, einer IP-Adresse oder einer URI, die in Detail-Metrik Metrikdaten gefunden wurden.

Markieren Sie einen Metrikwert im oberen Diagramm

Wählen Sie eine einzelne Zeile oder mehrere Zeilen aus, um die Diagrammdaten im oberen Diagramm auf der Seite mit den Detail-Metrik zu ändern. Zeigen Sie mit der Maus auf Datenpunkte im Diagramm, um weitere Informationen zu den einzelnen Datenpunkten anzuzeigen.

Per Schlüssel zu mehr Daten wechseln

Klicken Sie auf die Schlüsselnamen in der Einzelheiten Abschnitt, um detailliertere Metrikwerte zu sehen, aufgeschlüsselt nach anderen Schlüsseln. Klicken Sie für IP-Adresse oder Hostschlüssel auf einen Gerätenamen in der Tabelle, um zu einem Gerät Protokollseite, auf der der Verkehr und die Protokollaktivitäten angezeigt werden, die mit diesem Gerät verknüpft sind.

Passen Sie das Zeitintervall an und vergleichen Sie Daten aus zwei Zeitintervallen

Durch Ändern des Zeitintervalls können Sie Metrikdaten zu verschiedenen Zeiten in derselben Tabelle anzeigen und vergleichen. Weitere Informationen finden Sie unter Vergleichen Sie Zeitintervalle, um das Metrik Delta zu ermitteln.

Hinweis: Das globale Zeitintervall in der oberen linken Ecke der Seite enthält ein blaues Aktualisierungssymbol und einen grauen Text, der angibt, wann die Drilldown-Metriken zuletzt abgefragt wurden. Um die Metriken für das angegebene Zeitintervall neu zu laden, klicken Sie auf das Aktualisierungssymbol in der Anzeige von Global Zeitselektor. Weitere Informationen finden Sie unter Die neuesten Daten für ein Zeitintervall anzeigen.

Metrikdaten in Spalten sortieren

Klicken Sie auf die Spaltenüberschrift, um nach Metriken zu sortieren und anzuzeigen, welche Schlüssel den größten oder kleinsten Metrikwerten zugeordnet sind. Sortieren Sie beispielsweise nach der Verarbeitungszeit, um zu sehen, welche Kunden die längsten Ladezeiten der Website hatten.

Datenberechnung für Metriken ändern

Ändern Sie die folgenden Berechnungen für die in der Tabelle angezeigten Metrikwerte:

- Wenn die Tabelle eine Zählmetrik enthält, klicken Sie auf **Graf** in der Optionen Abschnitt im linken Bereich und wählen Sie dann **Durchschnittliche Rate**. Erfahren Sie mehr in der Rate oder Anzahl in einem Diagramm anzeigen Thema.
- Wenn die Tabelle eine Datensatzmetrik enthält, klicken Sie auf **Gemein** in der Optionen Abschnitt im linken Bereich und wählen Sie dann **Zusammenfassung**. Wenn du auswählst **Zusammenfassung**, Sie können den Mittelwert und die Standardabweichung anzeigen.

Daten exportieren

Klicken Sie mit der rechten Maustaste auf einen Metrikwert in der Tabelle, um eine PDF-, CSV- oder Excel-Datei herunterzuladen.

Ein zweites Mal mit einem Schlüsselfilter aufschlüsseln

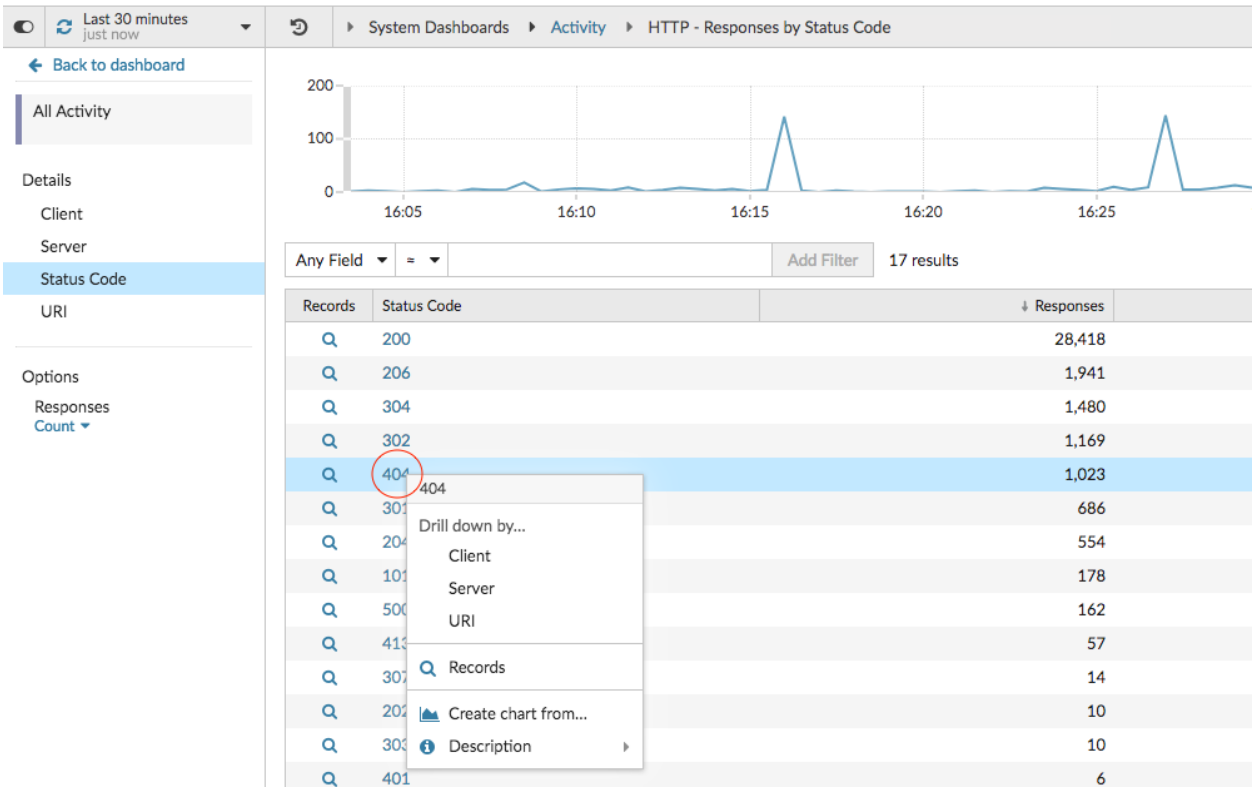
Nachdem Sie eine Top-Level-Metrik zunächst nach Schlüsseln aufgeschlüsselt haben, wird eine Detailseite mit einem Topnset von Metrik Werten, aufgeschlüsselt nach diesem Schlüssel. Sie können dann einen Filter erstellen, um einen zweiten Drilldown mit einem anderen Schlüssel durchzuführen. Sie können beispielsweise HTTP-Antworten nach Statuscode aufschlüsseln und dann erneut nach dem 404-Statuscode aufschlüsseln, um weitere Informationen zu den Servern, URIs oder Clients zu finden, die mit diesem Statuscode verknüpft sind.

Hinweis: Die Option, einen zweiten Drilldown durchzuführen, ist nur für bestimmte Topnsets verfügbar.

Die folgenden Schritte zeigen Ihnen, wie Sie von einem Diagramm aus einen Drilldown durchführen und dann von einer Detailseite mit Metriken aus erneut einen Drilldown durchführen:

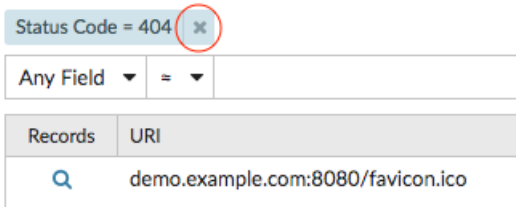
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einer Dashboard- oder Protokollseite.
3. Klicken Sie auf einen Metrikwert oder eine Metrikbezeichnung.
4. In der Drilldown nach... Abschnitt, wählen Sie einen Schlüssel aus.
   Eine Detailseite wird angezeigt.

5. Klicken Sie in der Tabelle auf einen Schlüssel, z. B. einen Statuscode oder eine Methode. (Der Schlüssel darf keine IP-Adresse oder kein Hostname sein.)
6. In der Drilldown nach... Wählen Sie im Abschnitt einen Schlüssel aus, wie in der folgenden Abbildung dargestellt.

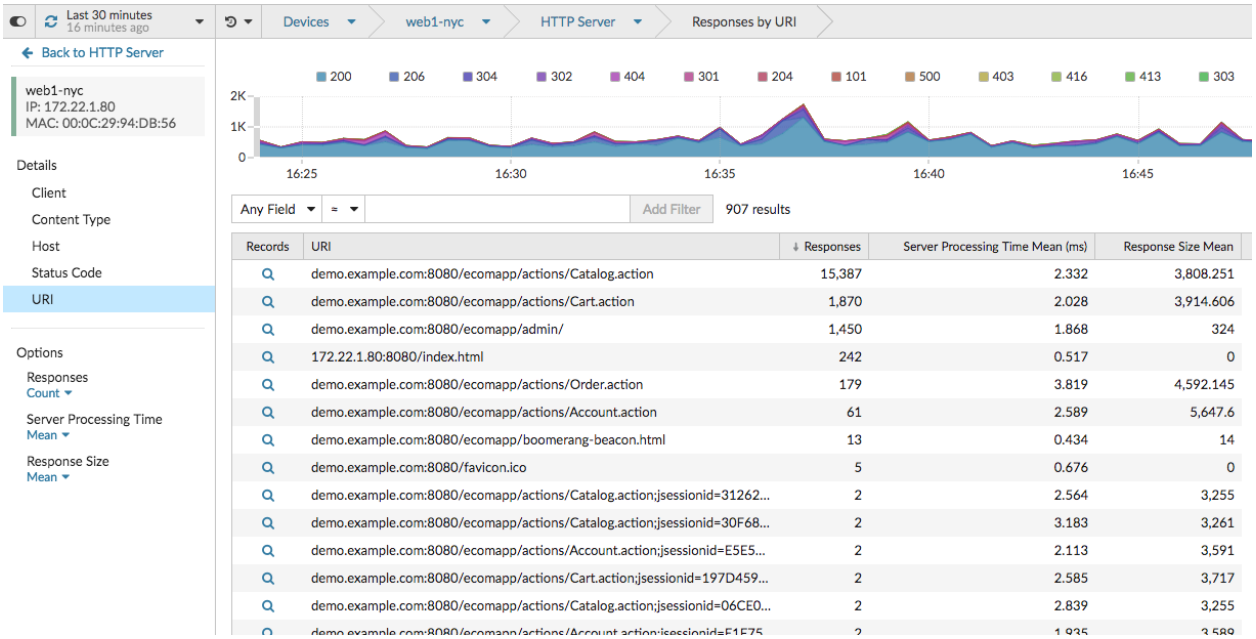


Der Schlüsselfilter wird über der Tabelle angezeigt. Sie können jetzt alle Detailmetriken anzeigen, die mit diesem einzelnen Schlüssel verknüpft sind.

7. Um diesen Filter aus der Tabelle zu entfernen und ihn dann auf das obere Diagramm anzuwenden, klicken Sie auf **x** Symbol, wie in der folgenden Abbildung dargestellt.



Der Filter im Diagramm bleibt bestehen, wenn Sie andere Schlüssel im Abschnitt Details auswählen.



Detailmetriken zu einem Diagramm hinzufügen

Wenn Sie schnell eine Reihe von Detailmetriken in einem Dashboard überwachen möchten, ohne dieselben Drilldown-Schritte wiederholt ausführen zu müssen, können Sie bei der Bearbeitung eines Diagramms in der Metric Explorer. In den meisten Diagrammen können bis zu 20 der wichtigsten Detailmetrikwerte nach Schlüsseln aufgeschlüsselt angezeigt werden. Ein Schlüssel kann eine Client-IP-Adresse, ein Hostname, eine Methode, ein URI, ein Referrer oder mehr sein. Tabellen- und Listen-Widgets können bis zu 200 Metrikwerte mit den wichtigsten Details anzeigen.

Ein Dashboard zur Überwachung des Webverkehrs kann beispielsweise ein Diagramm enthalten, in dem die Gesamtzahl der HTTP-Anfragen und -Antworten angezeigt wird. Sie können dieses Diagramm bearbeiten, um jede Metrik nach IP-Adresse aufzuschlüsseln und die Top-Talker zu sehen.

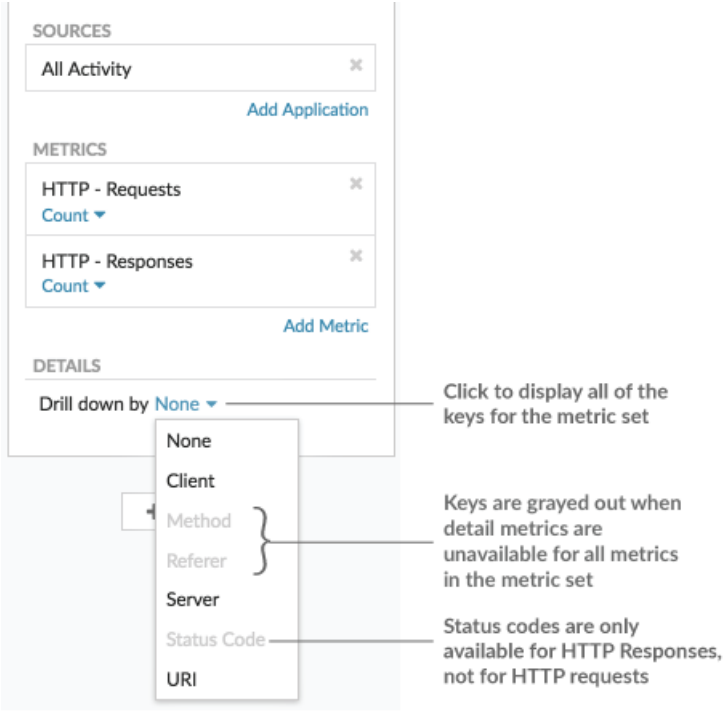
In den folgenden Schritten erfahren Sie, wie Sie ein vorhandenes Diagramm bearbeiten und anschließend Detailmetriken anzeigen können:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Navigieren Sie zu einer Dashboard- oder Protokollseite.
3. Klicken Sie auf den Diagrammtitel und wählen Sie dann **Bearbeiten**.
4. In der Einzelheiten Abschnitt, klicken **Drilldown nach *<None>*** , wo *<None>* ist der Name des Drilldown-Metrikschlüssels, der derzeit in Ihrem Diagramm angezeigt wird.
5. Wählen Sie einen Schlüssel aus der Drop-down-Liste aus.

Hinweis: Wenn Sie mehr als einen haben Quelle Die in Ihrem Metriksatz ausgewählten Quellen, z. B. zwei Geräte, werden beim Drilldown automatisch zu einer Ad-hoc-Quellengruppe zusammengefasst. Sie können die Auswahl nicht aufheben **Quellen kombinieren** Checkbox. Um Drilldown-Metriken für jede Quelle anzuzeigen, müssen Sie eine Quelle aus dem Metriksatz entfernen und dann auf **Quelle hinzufügen** um einen neuen Metriksatz zu erstellen.

Wenn detaillierte Metrikdaten für einen gemeinsamen Schlüssel für alle Metriken in einem Metriksatz verfügbar sind, wird der Schlüssel für die Detail-Metrik automatisch in der Dropdownliste angezeigt, wie in der folgenden Abbildung dargestellt. Wenn ein Schlüssel in der Liste ausgegraut ist, ist die mit diesem Schlüssel verknüpfte Detail-Metrik für alle Metriken in der oben genannten Metrik nicht

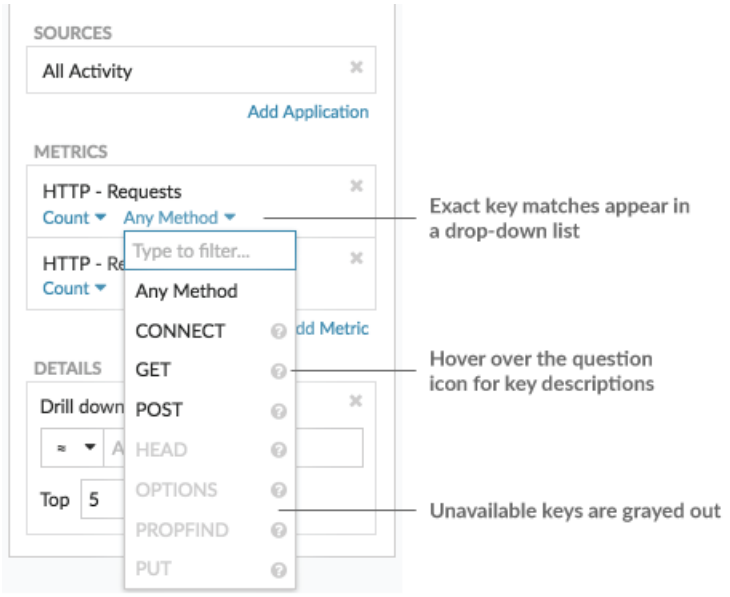
verfügbar. Beispielsweise sind Client-, Server- und URI-Daten sowohl für HTTP-Anfragen als auch für HTTP-Antwortmetriken im Metriksatz verfügbar.



6. Sie können Schlüssel mit einer ungefähren Übereinstimmung filtern, regulärer Ausdruck (Regex), oder führen Sie einen der folgenden Schritte durch, um eine exakte Übereinstimmung zu erzielen:
   - In der Filter Feld, wählen Sie **≈** Operator zur Anzeige von Schlüsseln nach ungefährer Übereinstimmung oder mit Regex. Sie müssen Schrägstriche mit Regex im Filter für ungefähre Treffer weglassen.

     Hinweis: Die **#** Die Filteroption zum Ausschließen von Ergebnissen ist nur verfügbar für Detailseiten. Wenn Sie Ergebnisse in einem Dashboard-Diagramm ausschließen möchten, erstellen Sie ein regulärer Ausdruck (Regex).
   - In der Filter Feld, wählen Sie **=** Operator zur Anzeige von Tasten nach exakter Übereinstimmung.
7. Optional: Geben Sie im oberen Ergebnisfeld die Anzahl der Schlüssel ein, die Sie anzeigen möchten. Diese Schlüssel werden die höchsten Werte haben.
8. Um eine Drilldown-Auswahl zu entfernen, klicken Sie auf **x** Ikone.

Hinweis: Sie können eine exakte Schlüsselübereinstimmung pro Metrik anzeigen, wie in der folgenden Abbildung dargestellt. Klicken Sie auf den Namen der Drilldown-Metrik (z. B. **Alle Methoden**), um einen bestimmten Metrik Drilldown-Key auszuwählen (z. B. `GET`) aus der Drop-down-Liste. Wenn ein Schlüssel grau erscheint (z. B. `PROPFIND`), sind Drilldown-Metrikdaten für diesen bestimmten Schlüssel nicht verfügbar. Sie können auch einen Schlüssel eingeben, der nicht in der Dropdownliste enthalten ist.


SOURCES
All Activity
Add Application
METRICS
HTTP - Requests
Count
Any Method
HTTP - Re
Count
dd Metric
DETAILS
Drill down
≈
Top
5
Type to filter...
Any Method
CONNECT
GET
POST
HEAD
OPTIONS
PROPFIND
PUT
Exact key matches appear in a drop-down list
Hover over the question icon for key descriptions
Unavailable keys are grayed out