

Filter für reguläre Ausdrücke

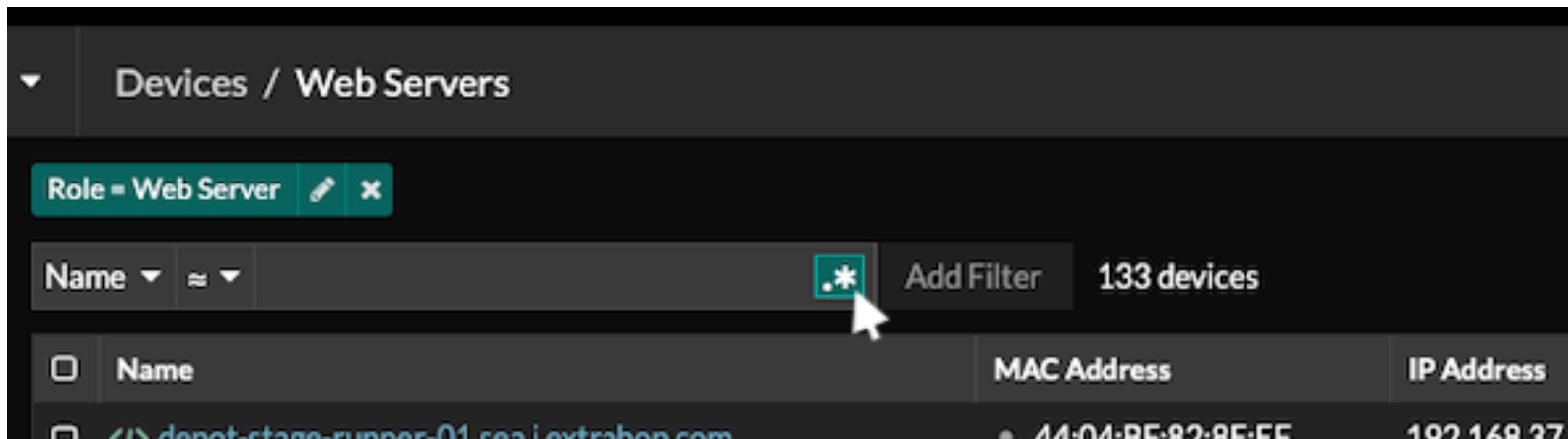
Veröffentlicht: 2024-09-25

Filtern Sie Ihre Suchergebnisse, indem Sie in bestimmte Suchfelder im gesamten ExtraHop-System Zeichenketten mit regulären Ausdrücken (Regex) schreiben. Sie können beispielsweise nach Parametern in einem Detail-Metrik Metrikschlüssel filtern, z. B. nach einer Zahl innerhalb einer IP-Adresse. Sie können auch filtern, indem Sie bestimmte Schlüssel oder eine Kombination von Schlüsseln aus Diagrammen ausschließen.

Regex-fähige Suchfelder verfügen über visuelle Indikatoren im gesamten System und akzeptieren die Standardsyntax.

Suchfelder mit einem Sternchen

Klicken Sie auf das Sternchen, um Regex-Zeichenfolgen zu aktivieren.

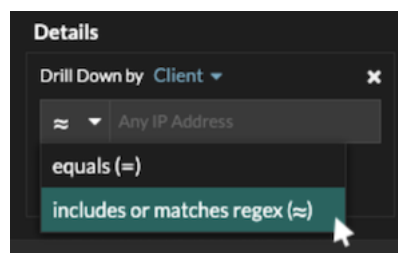


Dieser Feldtyp ist auf den folgenden Systemseiten verfügbar:

- Eine Tabelle mit Geräten filtern
- Filterkriterien für eine dynamische Gerätegruppe erstellen

Bestimmte Suchfelder mit einem Dreifeld-Operator

Klicken Sie auf das Operator-Dropdown-Menü, um die Regex-Option auszuwählen.

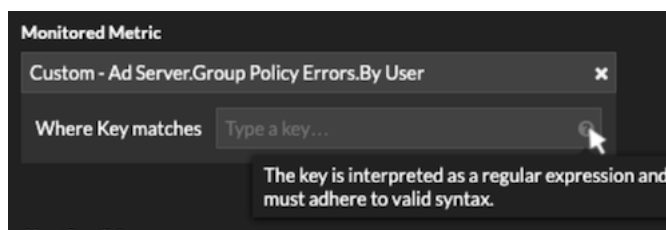


Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Ein Diagramm im Metric Explorer bearbeiten

Bestimmte Suchfelder mit einem Tooltip

Zeigen Sie mit der Maus auf den Tooltip im Feld, um zu sehen, wann Regex erforderlich ist.



Dieser Feldtyp ist auf der folgenden Systemseite verfügbar:

- Hinzufügen von Datensatzbeziehungen zu einer benutzerdefinierten Metrik

Die folgende Tabelle enthält Beispiele für die Standard-Regex-Syntax.

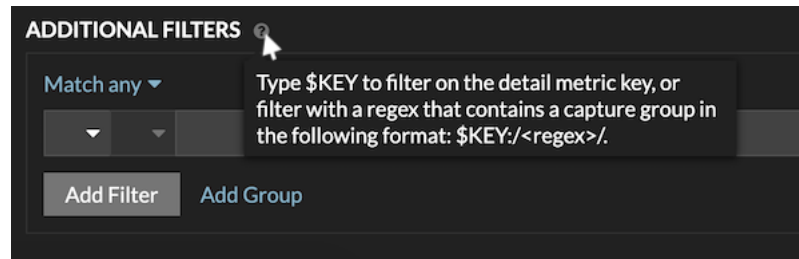
Diagrammszenario	Regex-Filter	So funktioniert's
Vergleichen Sie HTTP-Statuscodes 200 zu 404.	(200 404)	Das vertikale Balkensymbol () ist der OR-Operator. Dieser Filter entspricht 200, oder 404, oder beide Statuscodes.
Zeigt jeden HTTP-Statuscode an, der einen enthält 4.	[4]	Eckige Klammern ([und]) bezeichnen eine Reihe von Zeichen. Der Filter sucht nach jedem Zeichen innerhalb der Klammern, unabhängig von der Reihenfolge. Dieser Filter entspricht jedem Wert, der einen enthält 4 oder ein 1. Zum Beispiel kann dieser Filter zurückkehren 204, 400, 101, oder 201 Statuscodes.
Alles anzeigen 500HTTP-Statuscodes auf -Ebene.	^ [5]	Das Caret-Symbol (^) außerhalb der eckigen Klammern ([und]) bedeutet „beginnt mit“. Dieser Filter entspricht jedem Wert, der mit einem beginnt 5. Dieser Filter kann beispielsweise zurückkehren 500 und 502 Statuscodes.
Alles anzeigen 400 und 500 HTTP-Statuscodes auf -Ebene.	^ [45]	Mehrere Werte in eckigen Klammern ([und]) werden einzeln durchsucht, auch wenn ihnen das Caret-Symbol (^) vorangestellt ist. Dieser Filter sucht nicht nach Werten, die beginnen mit 45, entspricht aber allen Werten, die mit einem beginnen 4 oder 5. Zum Beispiel kann dieser Filter zurückkehren 400, 403, und 500 Statuscodes.
Zeigt alle HTTP-Statuscodes an, außer 200 Statuscodes auf -Ebene.	^ (?! 2)	Ein Fragezeichen (?) und Ausrufezeichen (!) geben Sie in Klammern einen auszuschließenden Wert an. Dieser Filter entspricht allen Werten außer Werten, die mit

Diagrammszenario	Regex-Filter	So funktioniert's
		einem beginnen 2. Zum Beispiel kann dieser Filter zurückkehren 400, 500, und 302 Statuscodes.
Zeigen Sie eine beliebige IP-Adresse mit einem 187.	187.	Spiele 1, 8, und 7 Zeichen in der IP-Adresse. Dieser Filter gibt keine IP-Adressen zurück, die auf 187 enden, da der letzte Punkt angibt, dass nach den Werten etwas stehen muss. Wenn Sie den Punkt als Literalwert durchsuchen möchten, müssen Sie ihm einen umgekehrten Schrägstrich (\) voranstellen.
Überprüfen Sie alle IP-Adressen, die enthalten 187.18.	187\ .18.	Spiele 187.18 und alles, was folgt. Die erste Periode wird wörtlich behandelt, da ihr ein umgekehrter Schrägstrich (\) vorausgeht. Die zweite Periode wird als Platzhalter behandelt. Dieser Filter gibt beispielsweise Ergebnisse für 187.18.0.0, 180.187.0.0, oder 187.180.0.0/16. Dieser Filter gibt keine Adresse zurück, die endet mit 187.18, weil der Platzhalter erfordert, dass Zeichen den angegebenen Werten folgen.
Zeigt eine beliebige IP-Adresse an, außer 187.18.197.150.	^(?!187\ .18\ .197\ .150)	Stimmt mit allem überein, außer 187.18.197.150, wo ^ (?!) gibt den auszuschließenden Wert an.
Schließt eine Liste bestimmter IP-Adressen aus.	^(?!187\ .18\ .197\ .15[012])	Stimmt mit allem überein, außer 187.18.197.150, 187.18.197.151, und 187.18.197.152, wo ^ (?!) gibt den auszuschließenden Wert an und die eckigen Klammern ([und]) geben mehrere Werte an.

Zusätzliche Filter

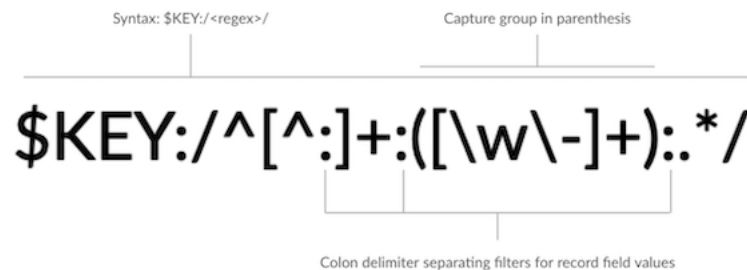
Wenn du [eine benutzerdefinierte Detail-Metrik erstellen](#)  Im Metrikkatalog können Sie dem Suchfeld **Zusätzliche Filter** im Abschnitt **Datensatzbeziehungen** eine erweiterte Regex-Syntax hinzufügen.

Der Tooltip wird angezeigt, nachdem Sie ausgewählt haben **Detailmetrik** und ist nicht verfügbar, wenn **Basismetrik** ist ausgewählt.



Die Regex-Syntax in diesem Feld muss die folgenden Anforderungen erfüllen:

- Wenn Ihr Schlüssel mehrere Werte enthält, muss Ihre Regex-Syntax eine einzelne Erfassungsgruppe enthalten. Eine Erfassungsgruppe wird durch Klammern gekennzeichnet. Ihre Capture-Gruppe bestimmt den Filterwert.



- Wenn Sie einen bestimmten Wert aus einem Detailmetrikschlüssel zurückgeben möchten, der mehrere Datensatzfeldwerte enthält, muss die Regex dieser Syntax folgen:

`$SCHLÜSSEL: / <regex> /`

Wenn Ihr Detailmetrikschlüssel beispielsweise `ipaddr:host:cipher` lautet und Sie nur den IP-Adresswert zurückgeben möchten, geben Sie Folgendes ein:

`$SCHLÜSSEL: / ^ ([^ :] +) : . + /`

- Wenn Ihr Schlüssel mehrere Datensatzfeldwerte enthält, werden die Werte durch ein Trennzeichen getrennt, das in dem Auslöser angegeben ist, der den Schlüssel generiert. Die Platzierung der Trennzeichen in Ihrer Regex-Syntax muss mit den Trennzeichen im Detailschlüssel übereinstimmen. Wenn Sie beispielsweise einen Schlüssel mit drei Werten haben, die durch ein Trennzeichen getrennt sind, das ein Doppelpunkt ist, müssen die drei Werte für den Schlüssel in Ihrer Regex-Syntax durch zwei Doppelpunkte getrennt werden.



Hinweis: Wenn Sie alle Datensatzfeldwerte in einem detaillierten Metrikschlüssel zurückgeben möchten, geben Sie ein `$SCHLÜSSEL`. Wenn Ihr Detailmetrikschlüssel beispielsweise `ipaddr:host:cipher` lautet, geben Sie Folgendes ein `$SCHLÜSSEL` im Suchfeld, um alle drei dieser Felddatensatzwerte (IP-Adresse, Hostname und TLS Verschlüsselungssuite) zurückzugeben.