Filtres à expressions régulières

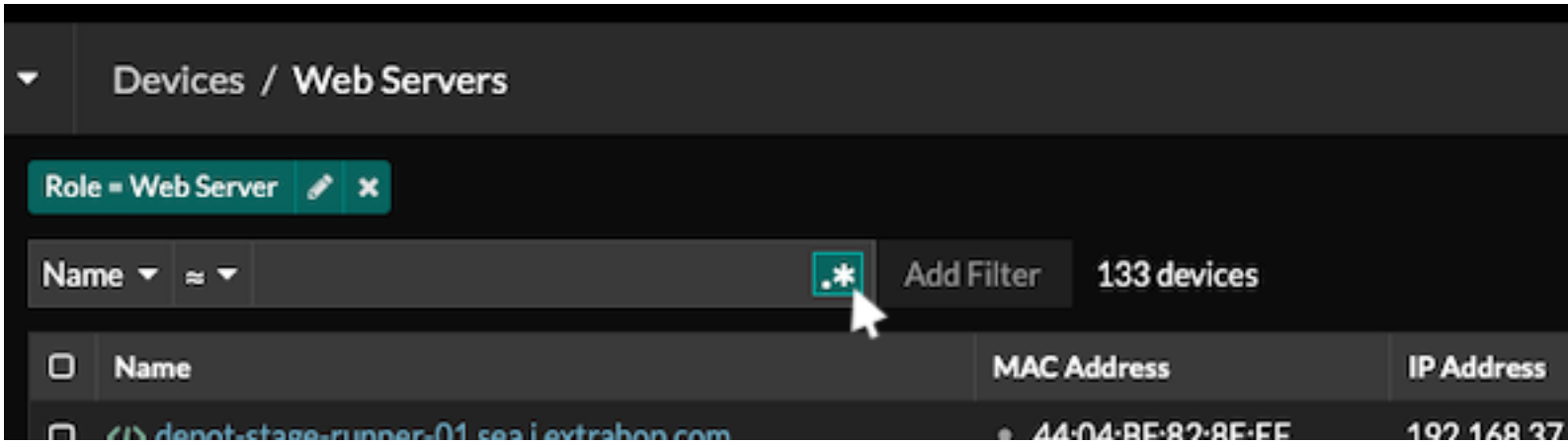
Publié: 2023-09-19

Filtrez les résultats de vos recherches en écrivant des chaînes d'expressions régulières (regex) dans certains champs de recherche du système ExtraHop. Par exemple, vous pouvez filtrer les paramètres d'une clé métrique détaillée, comme un nombre dans une adresse IP. Vous pouvez également filtrer en excluant des clés spécifiques ou une combinaison de clés des graphiques.

Les champs de recherche compatibles avec les expressions rationnelles sont dotés d'indicateurs visuels dans l'ensemble du système et acceptent une syntaxe standard.

Champs de recherche avec astérisque

Cliquez sur l'astérisque pour activer les chaînes regex.

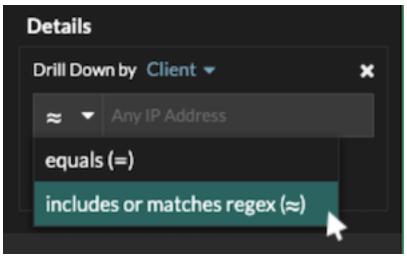


Ce type de champ est disponible dans les pages système suivantes :

- Filtrage d'un tableau de dispositifs
- Création de critères de filtrage pour un groupe dynamique de terminaux

Certains champs de recherche avec un opérateur tri-champ

Cliquez sur le menu déroulant de l'opérateur pour sélectionner l'option regex.

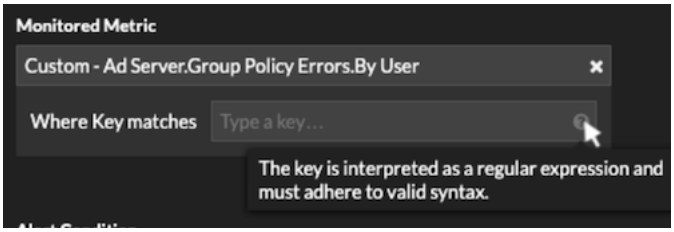


Ce type de champ est disponible à partir de la page système suivante :

- Modifier un graphique dans Metric Explorer

Certains champs de recherche avec une infobulle

Survolez l'infobulle dans le champ pour voir si une expression rationnelle est requise.



Ce type de champ est disponible à partir de la page système suivante : Ajouter des relations d'enregistrement à une métrique personnalisée :

- Ajouter des relations d'enregistrement à une métrique personnalisée

Le tableau suivant contient des exemples de la syntaxe standard des expressions rationnelles.

Scénario graphique	Filtre regex	Fonctionnement
Comparez les codes d'état HTTP `200` à `404`.	`(200|404)`	Le symbole de la barre verticale (	) est l'opérateur OR. Ce filtre correspond à `200`, ou `404`, ou aux deux codes d'état.
Affichez tout code d'état HTTP contenant un 4.	`[41]`	Les crochets ([et]) désignent une plage de caractères. Le filtre recherche tous les caractères à l'intérieur des crochets, quel que soit leur ordre. Ce filtre correspond à toute valeur contenant un 4 ou un 1. Par exemple, ce filtre peut renvoyer les codes d'état `204`, `400`, `101` ou `201`.
Afficher tous les codes d'état HTTP de niveau `500`.	`^[5]`	Le symbole de la caret (^) à l'extérieur des crochets ([et]) signifie "commence par". Ce filtre correspond à toute valeur commençant par 5. Par exemple, ce filtre peut renvoyer les codes d'état `500` et `502`.
Afficher tous les codes d'état HTTP de niveau `400` et `500`.	`^[45]`	Les valeurs multiples placées entre crochets ([et]) sont recherchées individuellement, même lorsqu'elles sont précédées du symbole de la caret (^). Ce filtre ne recherche pas les valeurs qui commencent par 45, mais correspond à toutes les valeurs qui commencent par 4 ou 5. Par exemple, ce filtre peut renvoyer les codes d'état `400`, `403` et `500`.
Affiche tous les codes d'état HTTP à l'exception des codes d'état de niveau `200`.	`^(?!2)`	Un point d'interrogation (?) et un point d'exclamation (!) entre parenthèses indiquent une valeur à exclure. Ce filtre correspond à toutes les valeurs à l'exception de celles commençant par 2. Par

Scénario graphique	Filtre regex	Fonctionnement
		exemple, ce filtre peut renvoyer les codes d'état `400`, `500` et `302`.
Afficher toute adresse IP commençant par `187.`	`187.`	Correspond aux caractères `1`, `8` et `7` de l'adresse IP. Ce filtre ne renvoie pas les adresses IP qui se terminent par 187, car le point final indique qu'il doit y avoir quelque chose après les valeurs. Si vous souhaitez rechercher le point en tant que valeur littérale, vous devez le faire précéder d'une barre oblique inverse (\ ).
Examinez toutes les adresses IP contenant `187.18.`	`187\.18.`	Correspond à `187.18` et à tout ce qui suit. Le premier point est traité littéralement parce qu'il est précédé d'une barre oblique inverse (\ ). Le deuxième point est traité comme un caractère générique. Par exemple, ce filtre renvoie les résultats pour `187.18.0.0`, `180.187.0.0`, ou `187.180.0.0/16`. Ce filtre ne renvoie pas d'adresse se terminant par `187.18`, car le caractère générique exige que les caractères suivent les valeurs spécifiées.
Afficher toute adresse IP à l'exception de `187.18.197.150`.	`^(?!187\.18\.197\.150)`	Correspond à tout ce qui n'est pas `187.18.197.150`, où `^(?!)` spécifie la valeur à exclure.
Exclure une liste d'adresses IP spécifiques.	`^(?!187\.18\.197\.15[012])`	Correspond à tout sauf `187.18.197.150`, `187.18.197.151`, et `187.18.197.152`, où `^(?!)`spécifie la valeur à exclure et les crochets ([et]) spécifient des valeurs multiples.

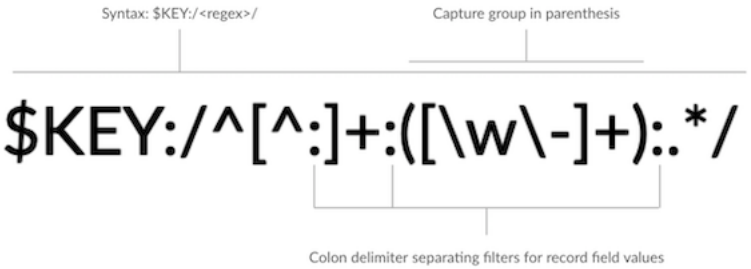
Filtres supplémentaires

Lorsque vous créez une mesure détaillée personnalisée à partir du catalogue de mesures, vous pouvez ajouter une syntaxe regex avancée au champ de recherche Filtres supplémentaires de la section Relations d'enregistrement.

L'infobulle apparaît après la sélection de la **métrique détaillée**et n'est pas disponible lorsque la **métrique de base** est sélectionnée.

La syntaxe des expressions rationnelles dans ce champ doit répondre aux exigences suivantes :

- Si votre clé contient plusieurs valeurs, votre syntaxe regex doit inclure un seul groupe de capture. Un groupe de capture est désigné par des parenthèses. Votre groupe de capture détermine la valeur du filtre.



- Si vous souhaitez renvoyer une valeur spécifique à partir d'une clé de métrique détaillée qui contient plusieurs valeurs de champ d'enregistrement, la syntaxe de recherche doit suivre cette syntaxe :

  `$KEY:/ <regex> /`

  Par exemple, si votre clé de métrique détaillée est ipaddr:host:cipher et que vous ne souhaitez renvoyer que la valeur de l'adresse IP, vous devez taper ce qui suit :

  `$KEY:/^([^ :]+) :.+/`
- Si votre clé contient plusieurs valeurs de champs d'enregistrement, les valeurs sont séparées par un délimiteur spécifié dans le déclencheur qui génère la clé. L'emplacement des délimiteurs dans votre syntaxe d'expressions rationnelles doit correspondre aux délimiteurs de la clé détaillée. Par exemple, si vous avez une clé comportant trois valeurs séparées par un délimiteur qui est un deux-points, les trois valeurs de la clé dans votre syntaxe de recherche doivent être séparées par deux deux-points.

Conseil: Si vous souhaitez renvoyer toutes les valeurs des champs d'un enregistrement dans une clé métrique détaillée, saisissez $KEY. Par exemple, si votre clé de métrique détaillée est ipaddr:host:cipher, tapez $KEY dans le champ de recherche pour obtenir les trois valeurs d'enregistrement de ce champ (adresse IP, nom d'hôte et suite de chiffrement SSL).