Filtres d'expressions régulières

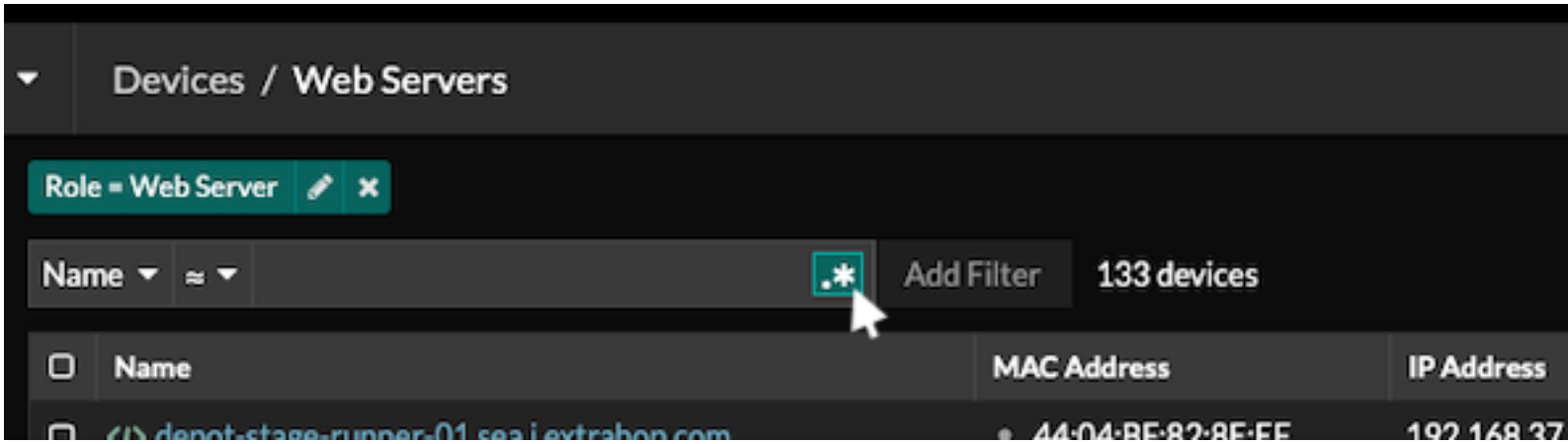
Publié: 2023-09-30

Filtrez les résultats de votre recherche 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 Regex comportent des indicateurs visuels dans l'ensemble du système et acceptent une syntaxe standard.

Champs de recherche marqués d'un astérisque

Cliquez sur l'astérisque pour activer les chaînes regex.

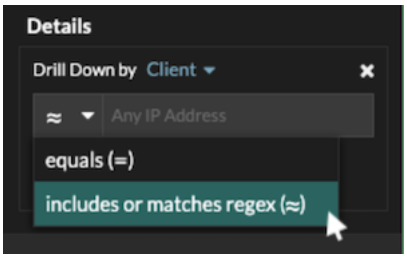


Ce type de champ est disponible sur les pages système suivantes :

- Filtrer un tableau d'appareils
- Création de critères de filtrage pour un groupe déquipements dynamique

Certains champs de recherche avec un opérateur à trois champs

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

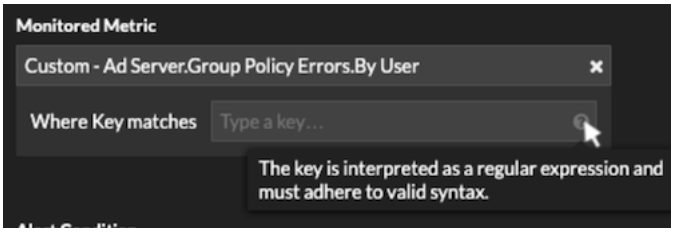


Ce type de champ est disponible sur la page système suivante :

- Modification d'un graphique dans l'explorateur de métriques

Certains champs de recherche avec une infobulle

Passez le pointeur de la souris sur l'infobulle dans le champ pour voir quand une expression régulière est requise.



Ce type de champ est disponible sur la page système suivante :

- Ajouter des relations d'enregistrement à une métrique personnalisée

Le tableau suivant inclut des exemples de syntaxe standard de regex.

Scénario graphique	Filtre Regex	Comment ça marche
Comparez les codes d'état HTTP `200` à `404`.	`(200|404)`	Le symbole en forme de barre verticale (|) est l'opérateur OR. Ce filtre correspond `200`, ou `404`, ou les deux codes de statut.
Afficher n'importe quel code d'état HTTP contenant un `4`.	`[41]`	Les crochets ([et]) désignent une série de caractères. Le filtre recherche tous les caractères entre crochets, quel que soit leur ordre. Ce filtre correspond à toute valeur contenant un `4` ou un `1`. Par exemple, ce filtre peut renvoyer `204`, `400`, `101`, ou `201` codes de statut.
Afficher tout `500`codes d'état HTTP au niveau -level.	`^ [5]`	Le symbole du curseur (^) situé entre crochets ([et]) signifie « commence par ». Ce filtre correspond à toute valeur commençant par un `5`. Par exemple, ce filtre peut renvoyer `500` et `502` codes de statut.
Afficher tout `400` et `500`codes d'état HTTP au niveau -level.	`^ [45]`	Plusieurs valeurs entre crochets ([et]) sont recherchées individuellement, même si elles sont précédées du symbole du curseur (^). Ce filtre ne recherche pas les valeurs commençant par `45`, mais correspond à toutes les valeurs commençant par un `4` ou `5`. Par exemple, ce filtre peut renvoyer `400`, `403`, et `500` codes de statut.
Afficher tous les codes d'état HTTP sauf `200`codes d' état de niveau -level.	`^ (? ! 2)`	Un point d'interrogation (?) et point d'exclamation (!) entre parenthèses spécifient une valeur à exclure. Ce filtre correspond à toutes les valeurs, à l'exception des valeurs commençant par un `2`. Par exemple, ce filtre peut

Scénario graphique	Filtre Regex	Comment ça marche
		renvoyer `400`, `500`, et `302` codes de statut.
Afficher n'importe quelle adresse IP avec `187.`	`187.`	Allumettes `1`, `8`, et `7` caractères de l'adresse IP. Ce filtre ne renverra pas les adresses IP se terminant par `187`, car la période de fin indique que quelque chose doit suivre les valeurs. Si vous souhaitez rechercher le point sous forme de valeur littérale, vous devez le faire précéder d'une barre oblique inverse (\).
Vérifiez toutes les adresses IP contenant `187.18.`	`187 \ ,18.`	Allumettes `187.18` et tout ce qui suit. La première période est traitée littéralement car elle est précédée d'une barre oblique inverse (\). La deuxième période est traitée comme un joker. 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 n'importe quelle adresse IP sauf `187.18.197.150`.	`^ (? ! 187 \ .18 \ .197 \ .150)`	Correspond à tout sauf `187.18.197.150`, où `^(?!)` indique la valeur à exclure.
Excluez 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 `^(?!)` indique la valeur à exclure et les crochets ([et]) indiquent plusieurs valeurs.

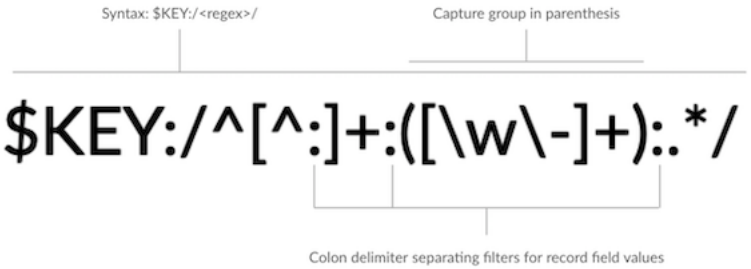
Filtres supplémentaires

Lorsque vous créer une métrique détaillée personnalisée à partir du catalogue de mesures, vous pouvez ajouter une syntaxe regex avancée au champ de recherche des filtres supplémentaires de la section Record Relationships.

L'infobulle apparaît une fois que vous avez sélectionné **Métrique détaillée** et n'est pas disponible lorsque **Métrique de base** est sélectionné.

La syntaxe regex de 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 métrique détaillée contenant plusieurs valeurs de champs d'enregistrement, l'expression régulière doit suivre la syntaxe suivante :

  `CLÉ $ :/ <regex> /`

  Par exemple, si votre clé métrique détaillée est ipaddr:host:cipher et que vous souhaitez uniquement renvoyer la valeur de l'adresse IP, vous devez saisir 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. Le placement des délimiteurs dans votre syntaxe regex doit correspondre aux délimiteurs de la clé de détail. Par exemple, si vous avez une clé avec trois valeurs séparées par un séparateur composé de deux points, les trois valeurs de la clé dans votre syntaxe regex doivent être séparées par deux points.

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