Disques

Publié: 2024-02-16

Les enregistrements sont des informations structurées sur les flux de transactions, de messages et de réseaux qui sont générées et envoyées depuis le système ExtraHop vers un espace de stockage des enregistrements. Une fois vos enregistrements collectés et stockés, vous pouvez les rechercher dans le système ExtraHop.

Les enregistrements sont collectés à deux niveaux de protocole : L3 et L7. Les enregistrements L3 (ou flux) indiquent les transactions de couche réseau entre deux appareils via le protocole IP. Les enregistrements L7 indiquent les transactions basées sur des messages (comme ActiveMQ, DNS et DHCP), transactionnelles (telles que HTTP, CIFS et NFS) et basées sur des sessions (telles que SSL et ICA).

Par exemple, si vous avez rencontré cinquante erreurs HTTP 503, les transactions HTTP associées contiendraient des informations sur l'URL, le serveur Web, le client qui a envoyé la demande, etc. Ces informations peuvent vous aider à identifier le problème sous-jacent.

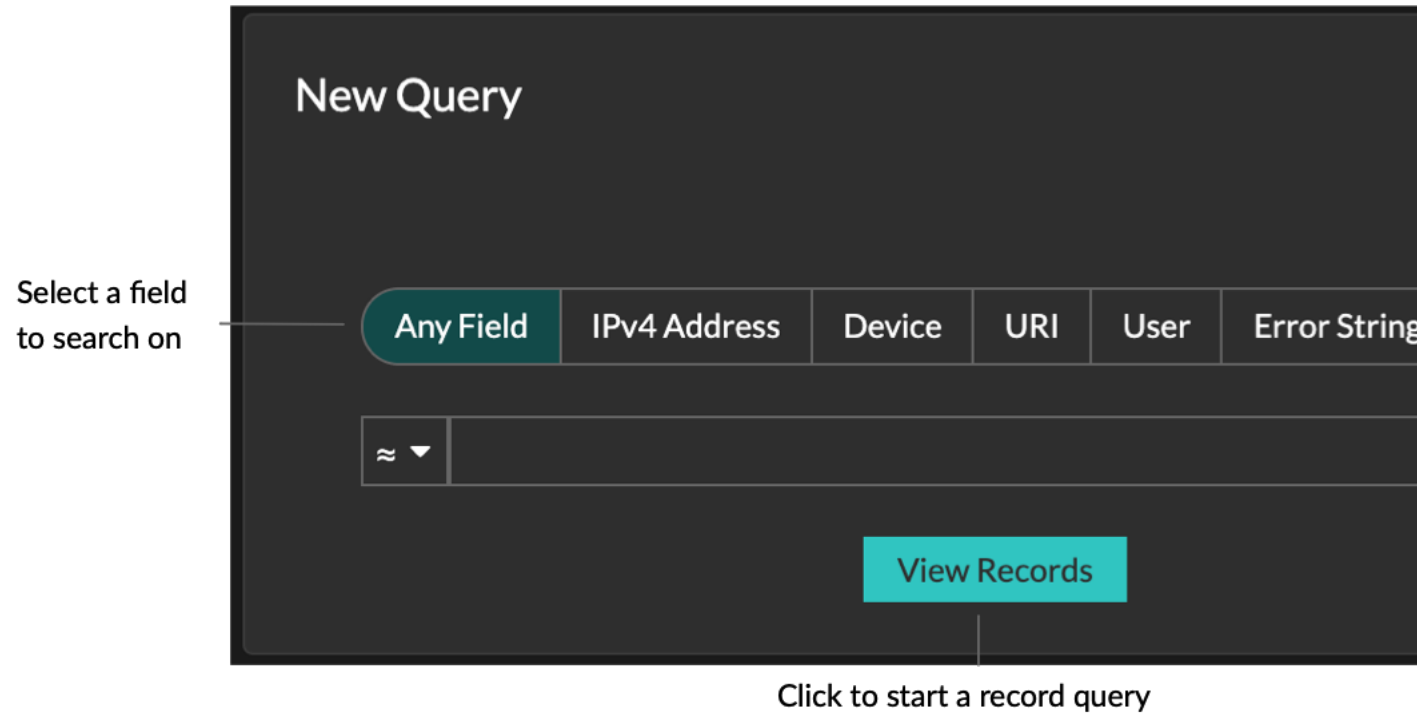
Vidéos Consultez la formation associée : Disques

Avant de commencer

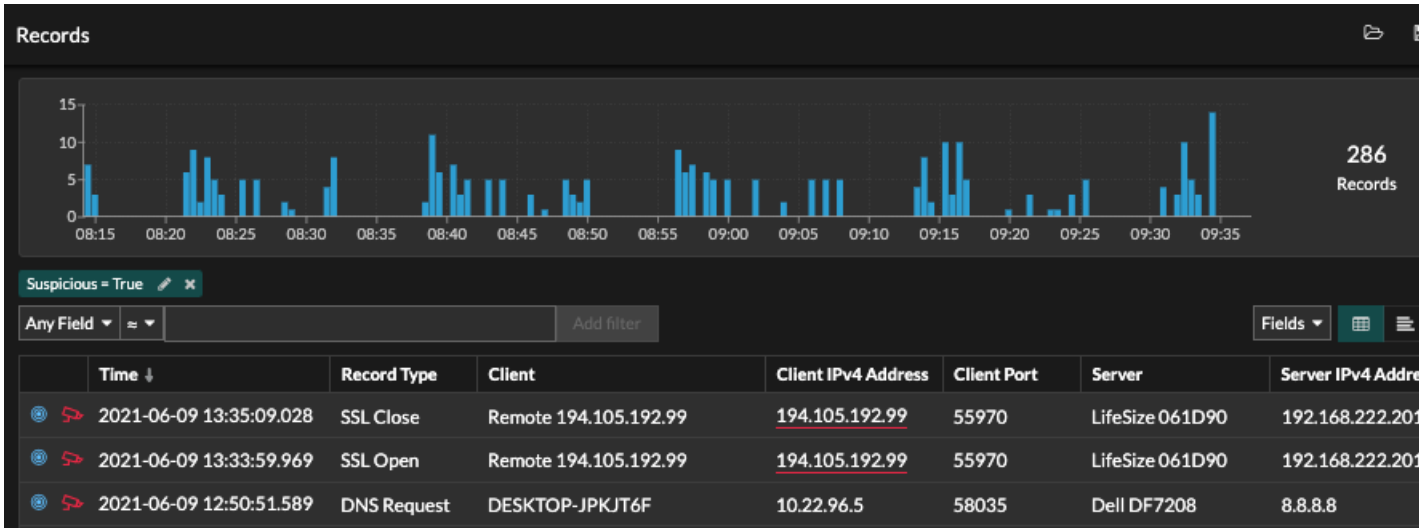
- Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un espace de stockage des enregistrements ExtraHop, Splunk, Google BigQuery, ou Balance à journaux CrowdStrike Falçon.
- Vous ne pouvez configurer qu'un seul espace de stockage des enregistrements pour le système ExtraHop.
- Votre système ExtraHop doit être configuré pour collecter et stocker enregistrements de flux ou records L7.

Navigation dans les enregistrements

Cliquez **Enregistrements** depuis le menu supérieur pour créer une nouvelle requête d'enregistrement. Sur la page Nouvelle requête, vous pouvez spécifier un filtre et un type d'enregistrement.



Les résultats apparaissent sur la page principale des enregistrements.



Note: Une requête peut générer des millions d'enregistrements en fonction de l'intervalle de temps et des critères de filtrage. Si une requête dépasse le nombre maximal de résultats, un nombre tronqué d' enregistrements apparaît. (espace de stockage des enregistrements ExtraHop uniquement.)

Voici quelques méthodes pour explorer les résultats des requêtes d'enregistrement :

- Dans le graphique des enregistrements, survolez un intervalle de temps pour afficher le nombre d'enregistrements, ou cliquez et faites glisser le pointeur sur le graphique pour limiter les résultats de la requête d'enregistrement à un intervalle de temps.

- Cliquez sur un nom d'hôte ou une adresse IP pour afficher les détails de l'équipement ou du point de terminaison externe.
- Les enregistrements contenant des adresses IP, des noms d'hôtes et des URI suspects apparaissent avec une icône de caméra rouge. Cliquez sur l'icône de la caméra pour voir renseignements sur les menaces pour l' enregistrement.
- Cliquez sur l'icône d'un paquet pour démarrer un requête par paquet qui est filtré par cet enregistrement.
- Les résultats des enregistrements apparaissent dans un tableau par défaut. Cliquez sur la vue tabulaire ou sur la vue détaillée  icônes pour passer de l'affichage de l'enregistrement à un autre.
- Une requête est automatiquement interrompue si le nombre d'octets d'enregistrement scannés ou renvoyés est extrêmement important. En cas de pause, la requête affiche les enregistrements les plus récents. Cliquez **Poursuivre la requête** pour reprendre la recherche.
- Cliquez sur le **Champs** liste déroulante pour ajouter des informations d'enregistrement supplémentaires à la vue des enregistrements.
- Dans l'affichage sous forme de tableau, cliquez et faites glisser les en-têtes de colonne pour organiser les informations d'enregistrement.
- Appliquer simple ou filtres avancés pour détecter des problèmes potentiels, tels que des délais de traitement trop longs ou des tailles de réponse inhabituelles.

Note: Pour créer une requête d'enregistrement pour une métrique personnalisée, vous devez d'abord définir la relation d'enregistrement par lier la métrique personnalisée à un type d'enregistrement.

Filtrez vos enregistrements à l'aide d'une simple requête

Vous pouvez filtrer les résultats de vos requêtes d'enregistrement de différentes manières afin de trouver la transaction exacte que vous recherchez. Les sections ci-dessous décrivent chaque méthode et présentent des exemples avec lesquels vous pouvez commencer pour vous familiariser.

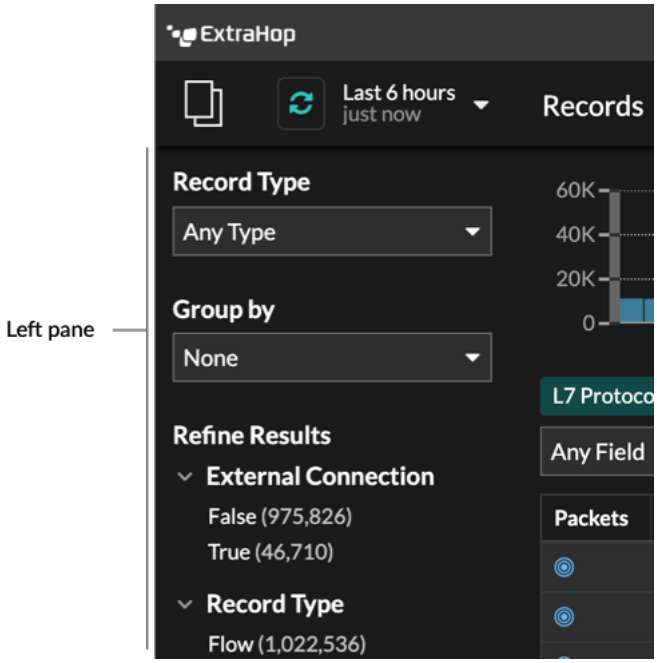
Si vous essayez de filtrer les enregistrements en fonction de critères simples (par exemple, si vous souhaitez que toutes les transactions HTTP proviennent d'un seul serveur qui a généré des 404), vous pouvez créer une requête simple de l'une des manières suivantes :

- Ajoutez un filtre ou affinez les résultats dans le volet de gauche
- Ajouter un filtre à partir du trichamp
- Ajouter un filtre directement à partir des résultats de l'enregistrement

Pour un filtrage complexe, voir Rechercher des enregistrements à l'aide d'un filtre avancé.

Filtrer les résultats des enregistrements dans le volet de gauche

Lorsque vous cliquez **Enregistrements** dans le menu supérieur, tous les enregistrements disponibles pour l'intervalle de temps sélectionné apparaissent. Vous pouvez ensuite filtrer dans le volet de gauche pour affiner vos résultats.



Le **Type d'enregistrement** le menu déroulant affiche une liste de tous les types d' enregistrements que votre système ExtraHop est configuré pour collecter et stocker. Un type d'enregistrement détermine les données collectées et stockées dans l'espace de stockage des enregistrements.

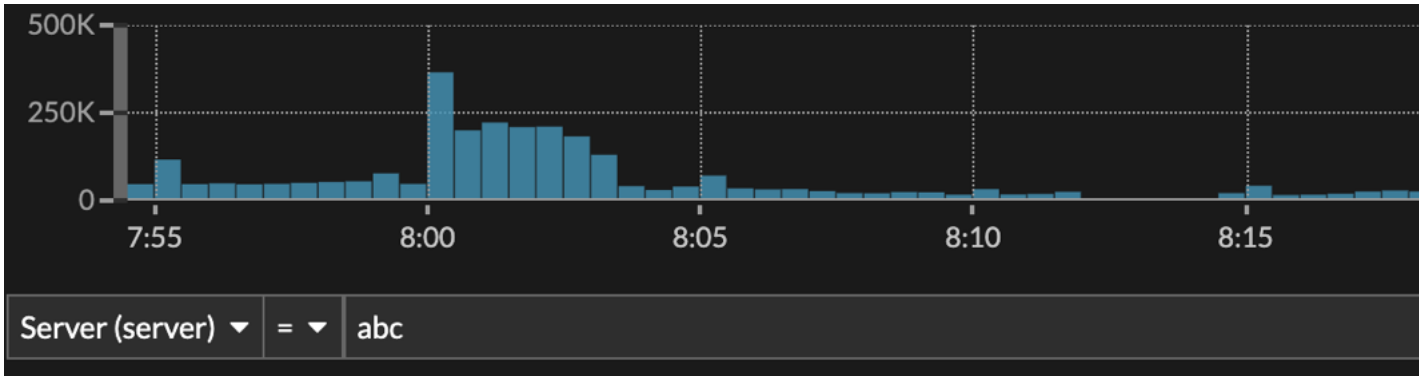
Note: Comme vous devez écrire un déclencheur pour collecter des enregistrements, vous devez trouver un moyen d' identifier le type de données que vous allez collecter. Il existe des types d'enregistrement intégrés, qui collectent tous les champs connus disponibles pour un protocole. Vous pouvez commencer par un type d' enregistrement intégré (tel que HTTP) et écrire un déclencheur pour collecter uniquement les champs de ce protocole qui vous intéressent (tels que l'URI et le code détat). Les utilisateurs expérimentés peuvent également créer un type d'enregistrement personnalisé s'ils ont besoin de collecter des informations propriétaires qui ne sont pas disponibles via un type d'enregistrement intégré.

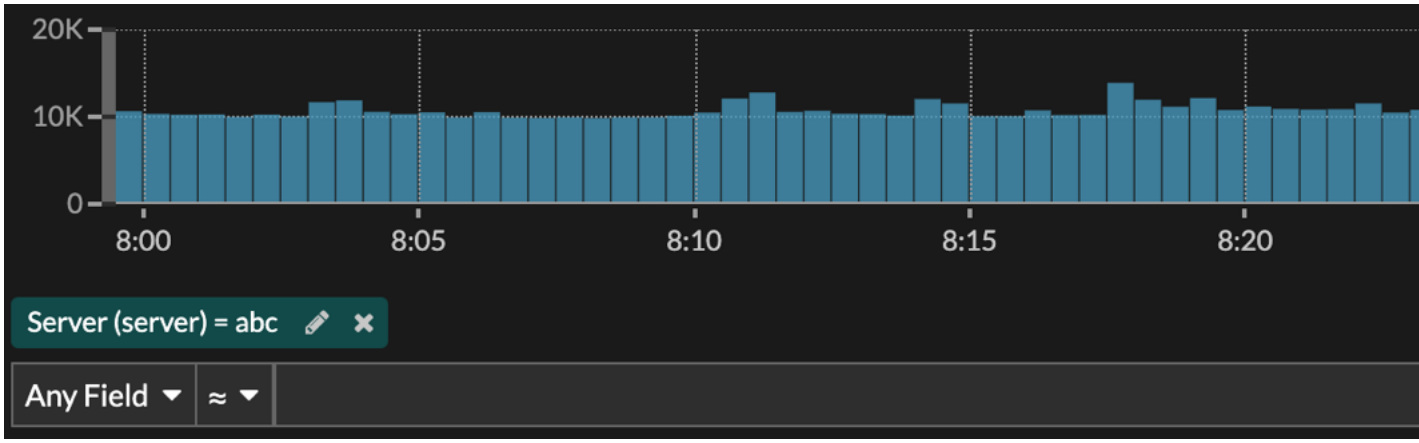
Le **Grouper par** la liste déroulante affiche une liste de champs permettant de filtrer davantage le type d'enregistrement.

Le **Affiner les résultats** cette section vous montre une liste de filtres d'enregistrement courants pour le type d'enregistrement sélectionné avec le nombre d'enregistrements correspondant au filtre entre parenthèses.

Filtrer les résultats des enregistrements via les trois champs

Sélectionnez un champ dans **N'importe quel domaine** menu déroulant (tel que Serveur), sélectionnez un opérateur (tel que le signe égal (=)), puis tapez un nom d'hôte. Cliquez **Ajouter un filtre**, et le filtre est ajouté au-dessus de la barre de filtre.





Vos résultats n'affichent que les enregistrements qui correspondent au filtre ; dans notre exemple, cela signifie que nous ne voyons que les résultats pour les transactions relatives au serveur nommé abc.

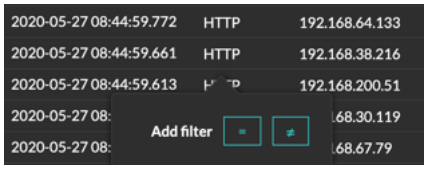
Les opérateurs suivants peuvent être sélectionnés en fonction du nom du champ sélectionné :

Opérateur	Descriptif
=	Égal
↓	N'est pas égal
≈	Comprend Si les enregistrements sont stockés dans un espace de stockage des enregistrements ExtraHop, l'opérateur d'inclusion fait correspondre les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche pour « www.extra » correspondrait à « www.extra.com » mais pas à « www.extrahop.com ». Pour tous les autres magasins de disques, l'opérateur includes fait correspondre les sous-chaînes, y compris les espaces et les signes de ponctuation. Par exemple, une recherche pour « www.extra » correspondrait à « www.extrahop.com », mais une recherche pour « www extra » ne correspondrait pas à « www.extrahop.com ».

Opérateur	Descriptif
	Les caractères Regex et les caractères génériques ne sont pas pris en charge.
≈/	Exclut Si les enregistrements sont stockés dans un espace de stockage des enregistrements ExtraHop, l'opérateur d'exclusion fait correspondre des mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche sur « extra » exclurait « www.extra.com » mais pas « www.extrahop.com ». Pour tous les autres magasins de disques, l'opérateur d'exclusion fait correspondre les sous-chaînes, y compris les espaces et les signes de ponctuation. Par exemple, une recherche sur « www.extra » exclurait « www.extrahop.com », mais une recherche sur « www extra » n'exclurait pas « www.extrahop.com ». Les caractères Regex et les caractères génériques ne sont pas pris en charge.
<	Inférieur à
≤	Inférieur ou égal à
>	Supérieur à
≥	Supérieur ou égal à
commence par	Commence par
existe	Existe
ne sort pas	N'existe pas

Filtrage direct à partir des résultats d'enregistrement

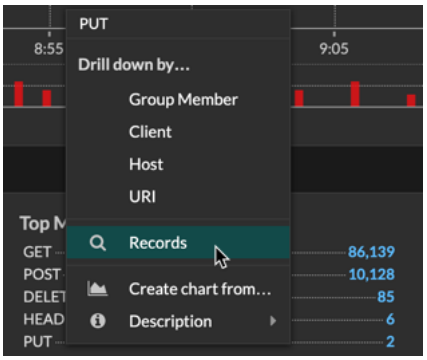
Vous pouvez sélectionner n'importe quelle entrée de champ affichée en mode tableau ou en mode détaillé dans les résultats de votre enregistrement, puis cliquer sur l'opérateur contextuel pour ajouter le filtre. Les filtres sont affichés sous le résumé du graphique (à l'exception du champ du type d'enregistrement, qui est modifié dans le volet de gauche).



Recherche d'enregistrements dans le système ExtraHop

- Tapez un terme de recherche dans le champ de recherche global en haut de l'écran et cliquez sur Rechercher des enregistrements pour lancer une recherche sur tous les enregistrements stockés.

- Sur la page de présentation de l'équipement, cliquez sur **Enregistrements** pour démarrer une requête filtrée par cet équipement.
- Sur la page de présentation d'un groupe déquipements, cliquez sur **Afficher les enregistrements** pour démarrer une requête filtrée en fonction de ce groupe déquipements.
- À partir d'une carte de détection, cliquez sur Afficher les enregistrements pour lancer une requête filtrée avec les transactions associées à la détection.
- Cliquez sur l'icône Records à partir d'un widget graphique, comme illustré dans la figure suivante.



- Cliquez sur l'icône Records à côté d'une métrique détaillée après avoir exploré une métrique de niveau supérieur. Par exemple, après avoir étudié les réponses HTTP par serveur, cliquez sur l'icône Enregistrements pour créer une requête pour les enregistrements contenant une adresse IP de serveur spécifique.